RSAC 2025 Conference

Many Voices. One Community.

SESSION ID: SBV-W09

WarGames 2027 & Maslow's Hierarchy of Needs as Hybrid Warfare Nears

Joshua Corman **@joshcorman** **@iamthecavalry** **@IST_org**
Founder, I am The Cavalry (dot org)
Executive in Residence, The Institute for Security & Technology (IST)
UnDisruptable27.org

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

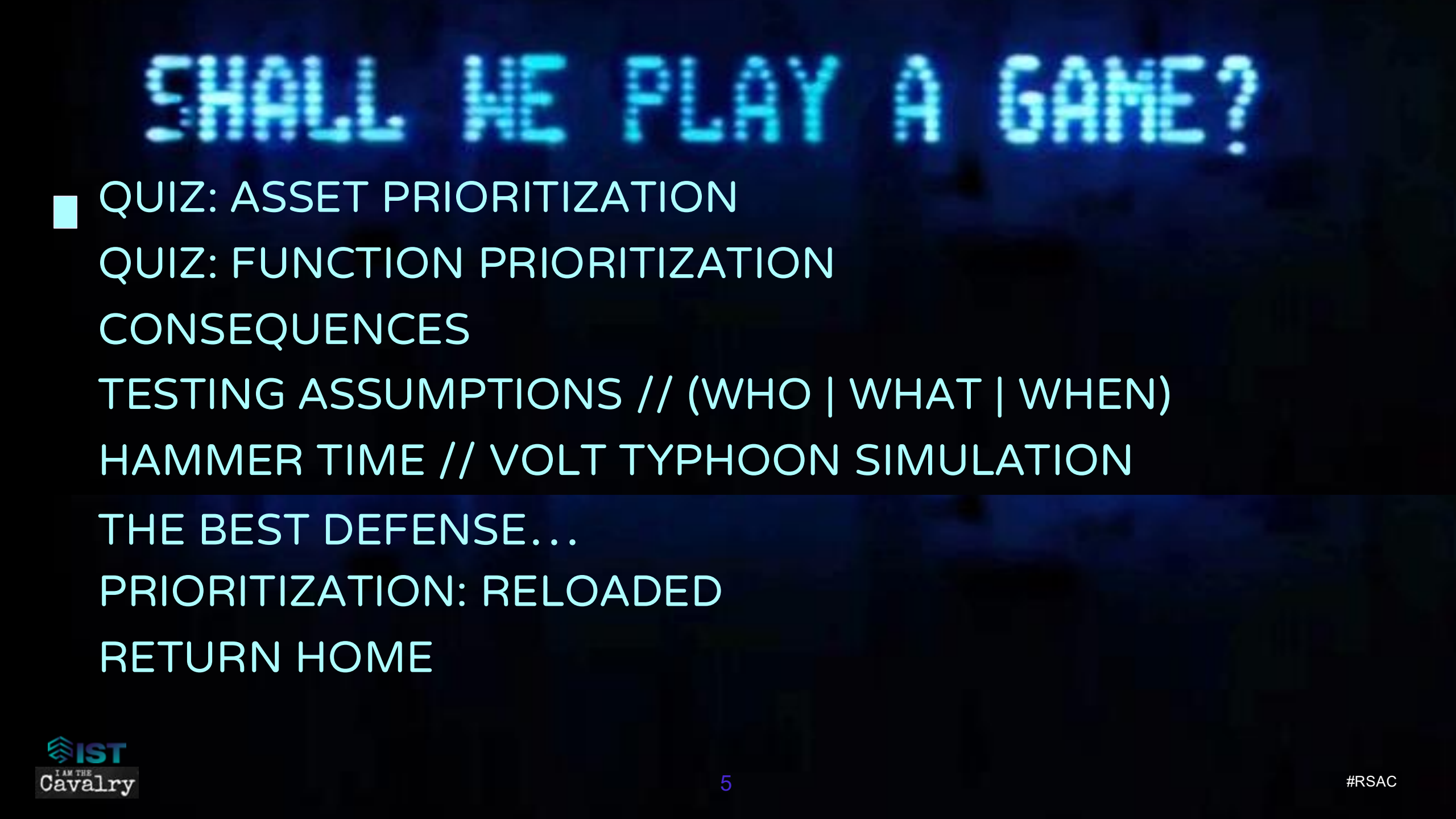
Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Abstract

Shall we play a game? This "choose your own adventure" session tackles the fast approaching reality of destructive cyberattacks on Lifeline Critical Functions like water, power, emergency care. The session will share the evidence, test assumptions, explore the art of the possible, and establish a sound hierarchy of needs enabling this talent pool to best serve the public good.

SHALL WE PLAY A GAME?



- QUIZ: ASSET PRIORITIZATION
- QUIZ: FUNCTION PRIORITIZATION
- CONSEQUENCES
- TESTING ASSUMPTIONS // (WHO | WHAT | WHEN)
- HAMMER TIME // VOLT TYPHOON SIMULATION
- THE BEST DEFENSE…
- PRIORITIZATION: RELOADED
- RETURN HOME

WHICH IS MORE IMPORTANT?

PCI

PAYMENT CARD DATA

PHI

PROTECTED HEALTH INFORMATION

WHICH IS MORE IMPORTANT?

IP

INTELLECTUAL PROPERTY

PHI

PROTECTED HEALTH INFORMATION

WHICH IS MORE IMPORTANT?

MEDICAL RECORDS

[CONFIDENTIALITY]

MEDICAL RECORDS

[AVAILABILITY]

WHICH IS MORE IMPORTANT?

YOUR WALLET

YOUR LIFE

WHICH IS MORE IMPORTANT?

THE NEEDS OF THE MANY

THE NEEDS OF THE FEW

WHICH IS MORE IMPORTANT?

PCI

PII

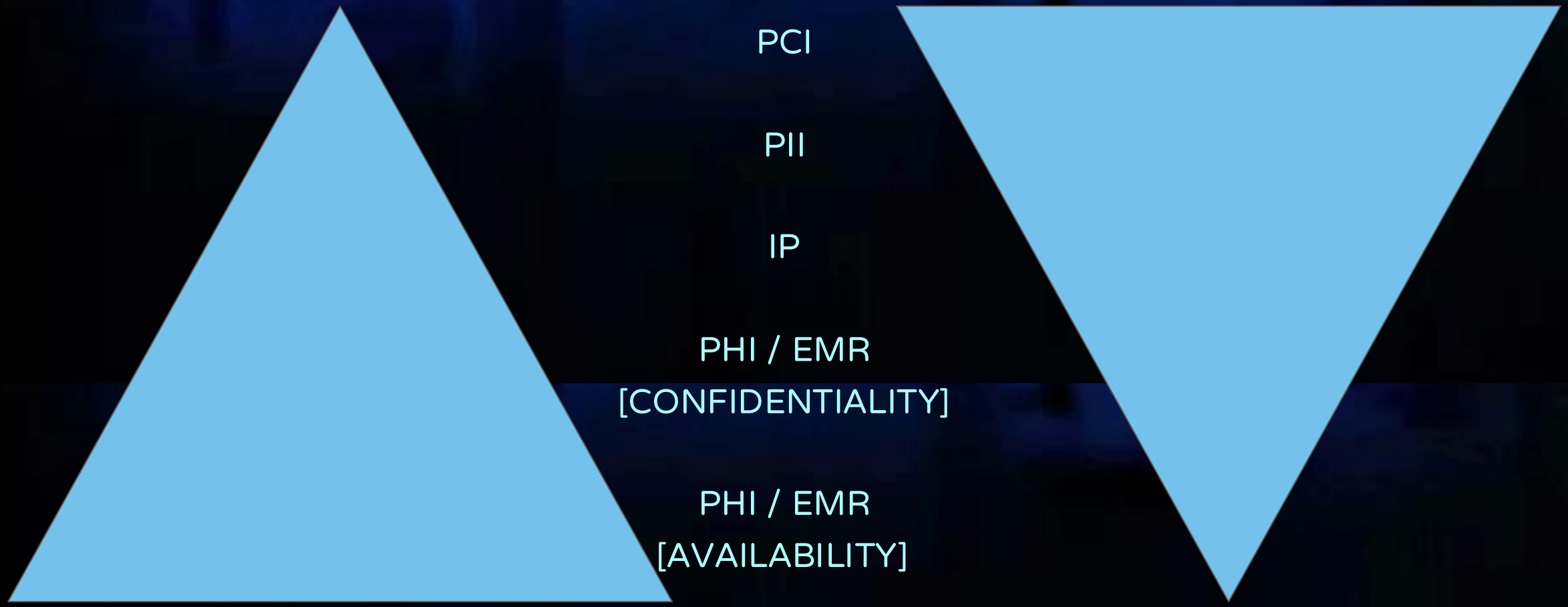
IP

PHI / EMR
[CONFIDENTIALITY]

PHI / EMR
[AVAILABILITY]

MASLOW'S

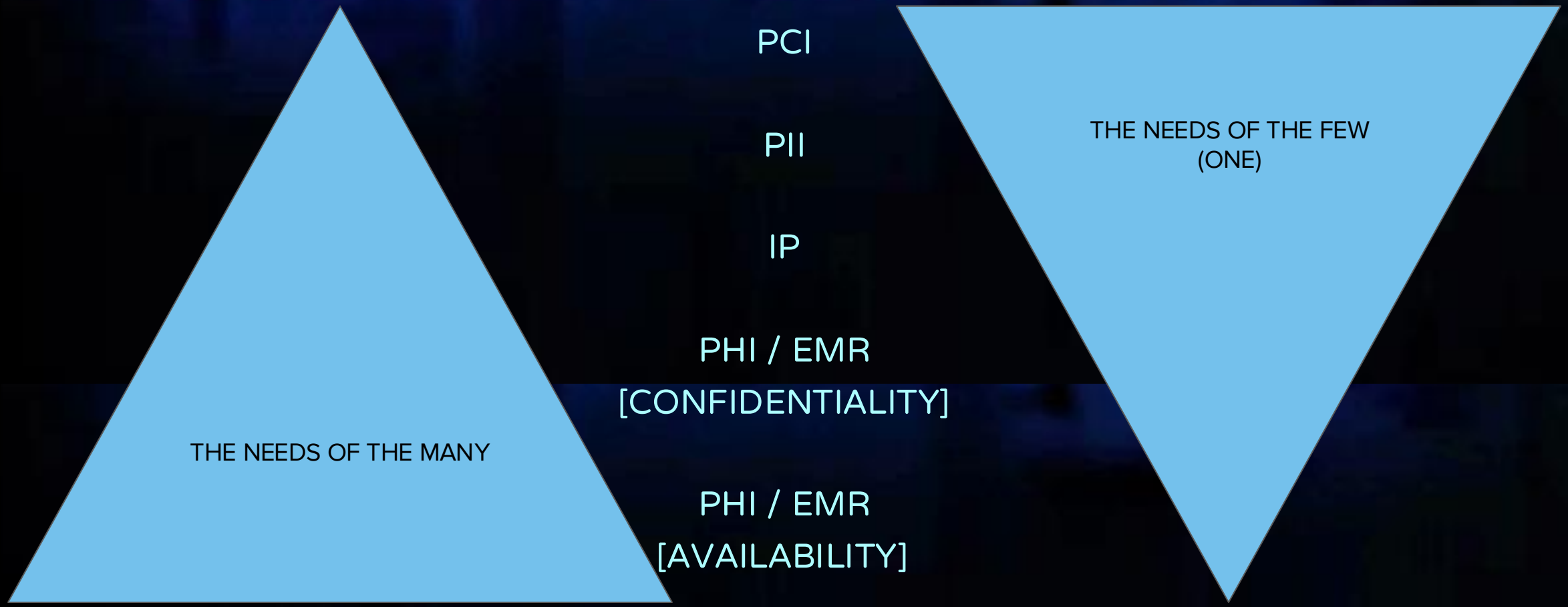
WHICH IS MORE IMPORTANT?



MASLOW'S

CYBERSECURITY

WHY?
WHICH IS MORE IMPORTANT?



MASLOW'S

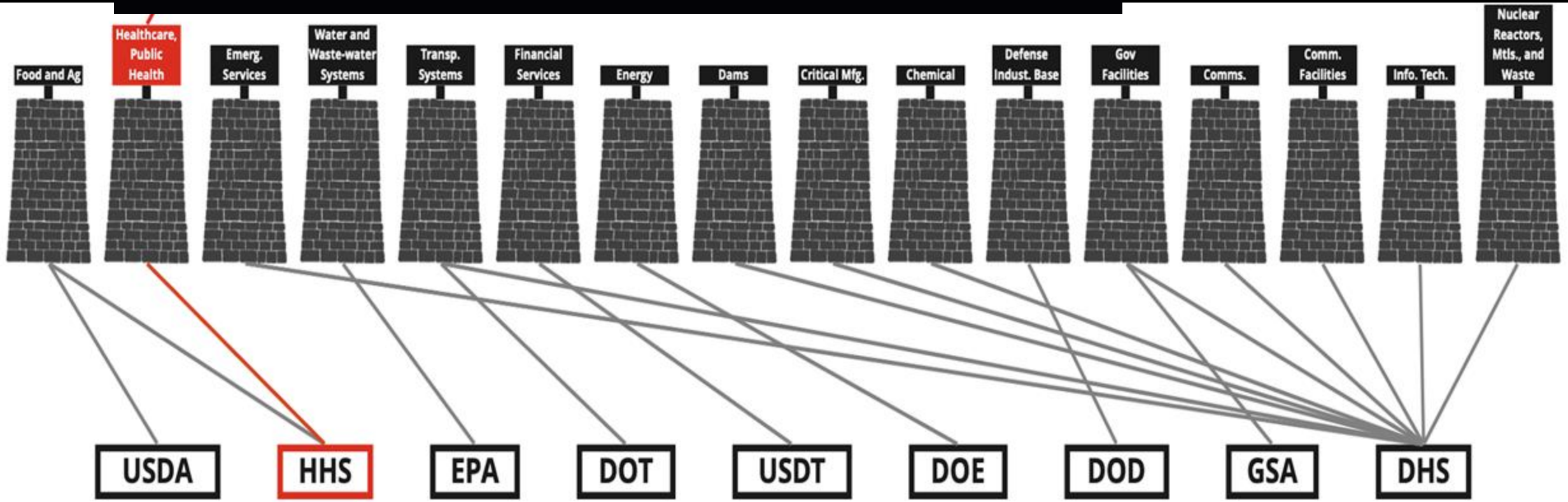
CYBERSECURITY

SHALL WE PLAY A GAME?

- QUIZ: ASSET PRIORITIZATION
- QUIZ: FUNCTION PRIORITIZATION
- CONSEQUENCES
- TESTING ASSUMPTIONS // (WHO | WHAT | WHEN)
- HAMMER TIME // VOLT TYPHOON SIMULATION
- THE BEST DEFENSE…
- PRIORITIZATION: RELOADED
- RETURN HOME

WHICH IS MORE IMPORTANT?

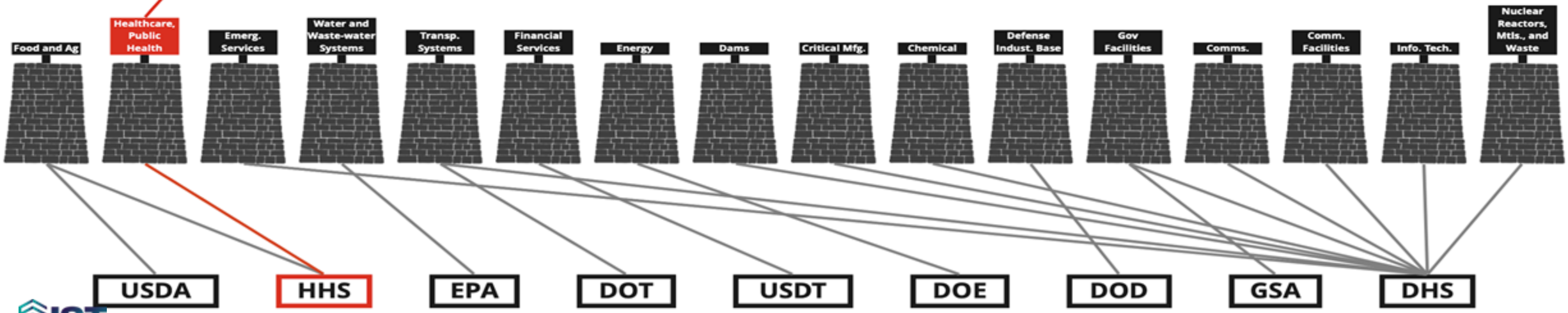
16 CRITICAL INFRASTRUCTURE SECTORS



IMG SRC: Ben Mosier & Josh Corman 2022

WHICH IS MORE IMPORTANT?

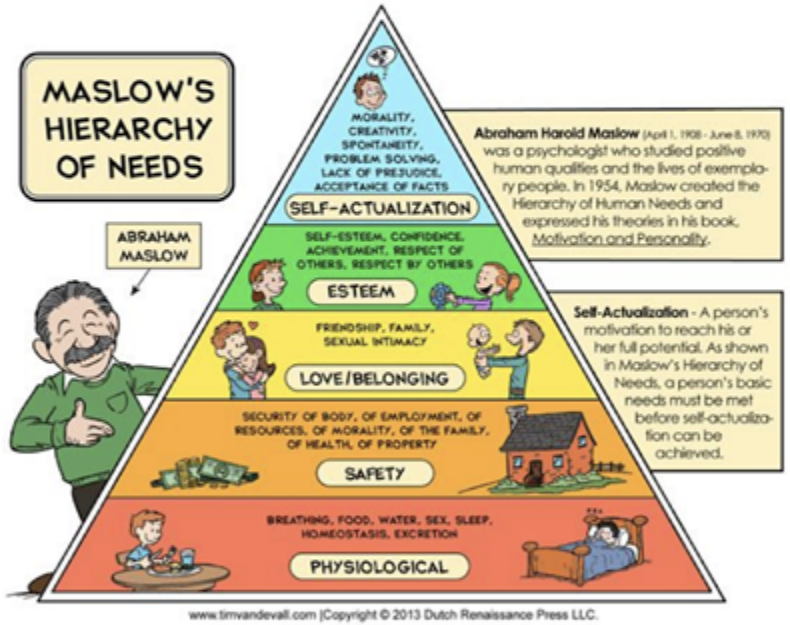
Operate Core Network	Distribute Electricity	Conduct Elections	Provide Medical Care	Provide Capital Markets and Investment Activities	Exploration and Extraction Of Fuels	Provide Housing	Provide Cable Access Network Services	Maintain Supply Chains	Educate and Train	Provide Public Safety	Provide Funding and Liquidity Services	Fuel Refining and Processing Fuels	Provide Information Technology Products and Services
Provide Internet Based Content, Information, and Communication Services	Transmit Electricity	Maintain Access to Medical Records	Store Fuel and Maintain Reserves	Provide Insurance Services	Generate Electricity	Provide Internet Routing, Access, and Connection Services	Transport Cargo and Passengers by Air	Manage Wastewater	Develop and Maintain Public Works and Services	Provide Payment, Clearing, and Settlement Services	Manufacture Equipment	Provide Materiel and Operational Support to Defense	Provide Positioning, Navigation, and Timing Services
Transport Cargo and Passengers by Rail	Perform Cyber Incident Management Capabilities	Enforce Law	Provide Wholesale Funding	Produce and Provide Agricultural Products and Services	R&D	Provide Radio Broadcast Access Network Services	Transport Cargo and Passengers by Road	Preserve Constitutional Rights	Manage Hazmat.	Support Community Health	Supply Water	Provide Satellite Access Network Services	Transport Cargo and Passengers by Vessel
Provide and Maintain Infrastructure	Operate Government	Produce and Provide Human and Animal Food Products and Services	Provide Wireless Access Network Services	Transport Materials by Pipeline	Provide Consumer and Commercial Banking Services	Prepare for and Manage Emergencies	Produce Chemicals	Provide Wireline Access Network Services	Transport Passengers by Mass Transit	Provide Identity Management and Associated Trust Support Services	Protect Sensitive Information	Provide Metals and Materials	



IST
I AM THE Cavalry

IMG SRC: Ben Mosier & Josh Corman 2022

*positions illustrative, not definitive


MASLOW'S HIERARCHY OF NEEDS
ABRAHAM MASLOW
MORALITY, CREATIVITY, SPONTANEITY, PROBLEM SOLVING, LACK OF PREJUDICE, ACCEPTANCE OF FACTS
SELF-ACTUALIZATION
SELF-ESTEEM, CONFIDENCE, ACHIEVEMENT, RESPECT OF OTHERS, RESPECT BY OTHERS
ESTEEM
FRIENDSHIP, FAMILY, SEXUAL INTIMACY
LOVE/BELONGING
SECURITY OF BODY, OF EMPLOYMENT, OF RESOURCES, OF MORALITY, OF THE FAMILY, OF HEALTH, OF PROPERTY
SAFETY
BREATHING, FOOD, WATER, SEX, SLEEP, HOMEOSTASIS, EXCRETION
PHYSIOLOGICAL
Abraham Harold Maslow (April 1, 1908 - June 8, 1970) was a psychologist who studied positive human qualities and the lives of exemplary people. In 1954, Maslow created the Hierarchy of Human Needs and expressed his theories in his book, Motivation and Personality.
Self-Actualization - A person's motivation to reach his or her full potential. As shown in Maslow's Hierarchy of Needs, a person's basic needs must be met before self-actualization can be achieved.
www.timvandevall.com |Copyright © 2013 Dutch Renaissance Press LLC.

IST
I AM THE Cavalry

IMG SRC: Ben Mosier & Josh Corman 2022

WHICH IS MORE IMPORTANT?

YOUR WALLET

YOUR LIFE

WHICH IS MORE IMPORTANT?

SUPPORT BANKING

PROVIDE FUEL

WHICH IS MORE IMPORTANT?

PROVIDE ELECTRICITY

PROVIDE FOOD

WHICH IS MORE IMPORTANT?

PROVIDE WATER

PROVIDE FOOD

WHICH IS MORE IMPORTANT?

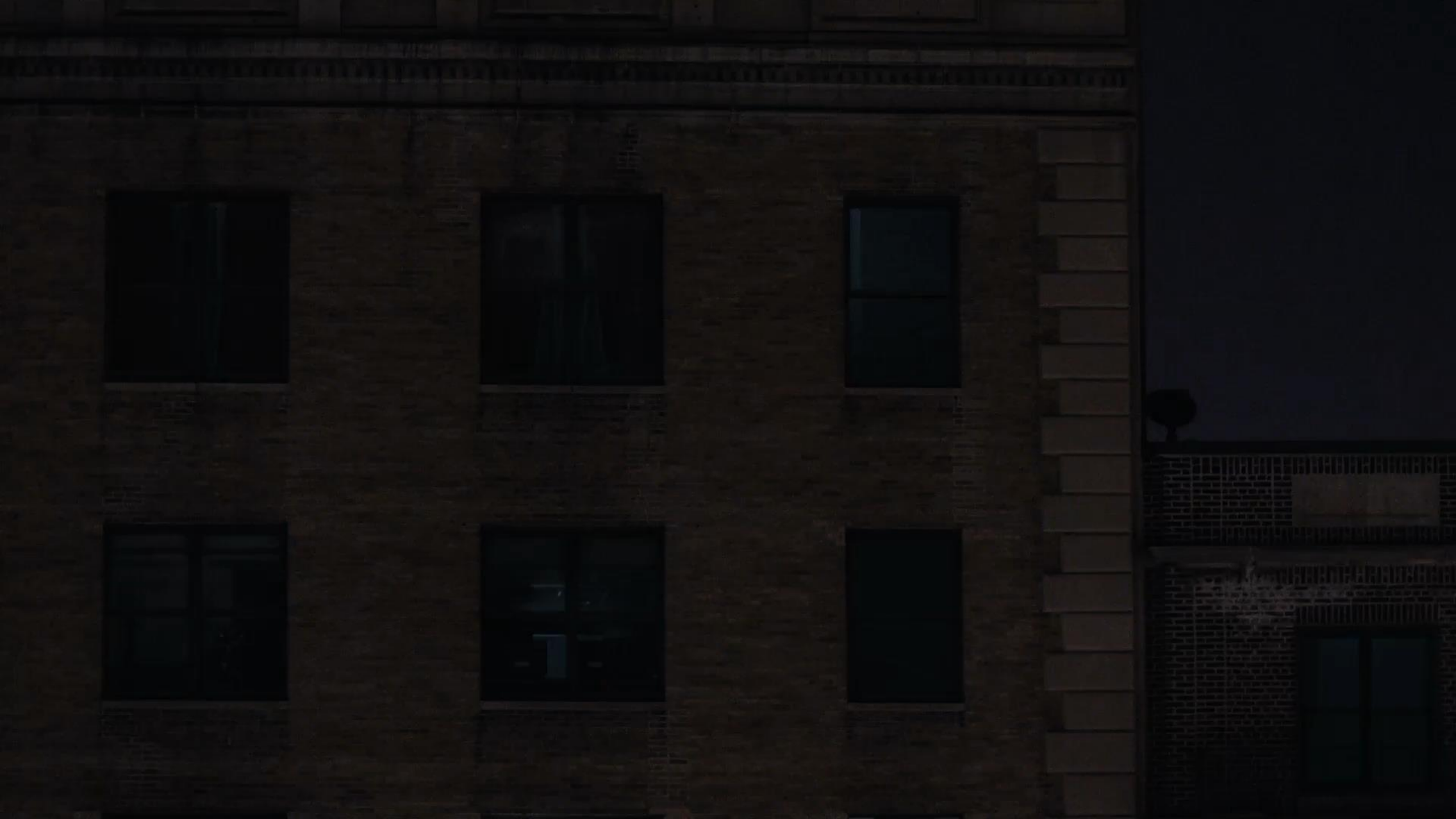
PROVIDE WATER

PROVIDE MEDICAL CARE

WHICH IS MORE IMPORTANT?

PROTECT SENSITIVE INFORMATION [PHI]

PROVIDE MEDICAL CARE



https://www.cisa.gov/sites/default/files/publications/CISA_Insight_Provide_Medical_Care_Sep2021.pdf

CISA INSIGHTS

Provide Medical Care is in Critical Condition: Analysis and Stakeholder Decision Support to Minimize Further Harm

September 2021

CRITICAL INFRASTRUCTURE DECISION SUPPORT

By late September, at least four states have declared Crisis Standards of Care (CSC), and an additional eight have delayed elective surgeries and/or are at risk of enacting CSC. Patient diversions across state lines further punctuate the dynamic we outlined in the Cascading failures model (see page 7).

As the COVID-19 pandemic reaches another phase, with increased and protracted strains on the nation's critical infrastructure and related National Critical Functions such as *Provide Medical Care,* CISA is undertaking a renewed push for cyber preparedness and resilience, as well as decision support for stakeholders within critical infrastructure sectors. Over time, we find these original insights increasingly valuable, and in service of timely decision support, we offer them to you in their original form. As British statistician George E. P. Box noted, "All models are wrong, but some are useful." We hope that these models and insights are useful to you and stimulate additional discussion and exploration for mutual benefit.

This CISA Insight will speak to:

- Analysis and insights into strains on the nation's critical infrastructure, specifically through impacts to the National Critical Function *Provide Medical Care,*
- The compounding risks and harms that apply to all critical infrastructure sectors and the 55 National Critical Functions, through impact to essential critical infrastructure workers, and
- Our intention to share our preliminary analysis, enable decision support, and assist in risk reduction across multiple stakeholders and critical infrastructure sectors.

https://www.cdc.gov/mmwr/volumes/70/wr/mm7046a5.htm?s_cid=mm7046a5_w

Morbidity and Mortality Weekly Report (*MMWR*)

Impact of Hospital Strain on Excess Deaths During the COVID-19 Pandemic — United States, July 2020–July 2021

Weekly / November 19, 2021 / 70(46);1613–1616

Geoffrey French, MA[1]; Mary Hulse, MPA[1]; Debbie Nguyen[2]; Katharine Sobotka[2]; Kaitlyn Webster, PhD[2]; Josh Corman[1]; Brago Aboagye-Nyame[2]; Marc Dion[2]; Moira Johnson[2]; Benjamin Zalinger, MA[2]; Maria Ewing[3] (View author affiliations)

View suggested citation

Summary

What is already known about this topic?

COVID-19 surges have stressed hospital systems and negatively affected health care and public health infrastructures and national critical functions.

What is added by this report?

The conditions of hospital strain during July 2020–July 2021, which included the presence of SARS-CoV-2 B.1.617.2 (Delta) variant, predicted that intensive care unit bed use at 75% capacity is associated with an estimated additional 12,000 excess deaths 2 weeks later. As hospitals exceed 100% ICU bed capacity, 80,000 excess deaths would be expected 2 weeks later.

What are the implications for public health practice?

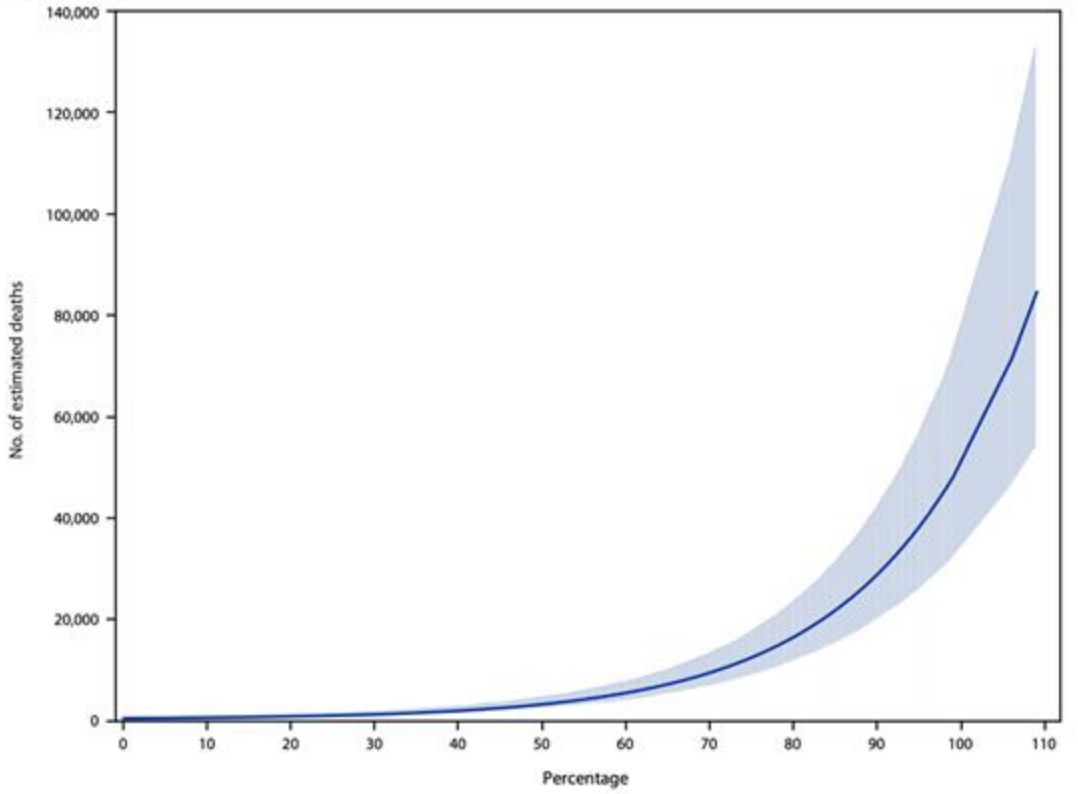
State, local, tribal, and territorial leaders could evaluate ways to reduce strain on public health and health care infrastructures, including implementing interventions to reduce overall disease prevalence such as vaccination and other prevention strategies, and ways to expand or enhance capacity during times of high disease prevalence.

Article Metrics
Altmetric:
Citations:
Views:
Views equals page views plus PDF downloads
Metric Details

Figure
References
Related Materials
PDF [319K]

Surges in COVID-19 cases have stressed hospital systems, negatively affected health care and public health infrastructures, and degraded national critical functions (*1*,*2*). Resource limitations, such as available hospital space, staffing, and supplies led some facilities to adopt crisis standards of care, the most extreme operating condition for hospitals, in which the focus of medical decision-making shifted from achieving the best outcomes for individual patients to addressing the immediate care needs of larger groups of patients (*3*). When hospitals deviated from conventional standards of care, many preventive and elective

FIGURE. Estimated number of excess deaths* 2 weeks after corresponding percentage of adult intensive care unit bed occupancy — United States, July 2020–July 2021



* Upper and lower boundaries of shaded area indicate 95% CIs.

Cybersecurity & Infrastructure Security Agency, unpublished data, 2021). As hospitals exceed 100% ICU bed capacity, 80,000 (95% CI = 53,576–132,765) excess deaths would be

health care and public health sectors, with excess deaths emerging in the weeks after a surge in COVID-19 hospitalizations. The results of this study support a larger body of evidence

https://www.cisa.gov/publication/provide-medical-care-critical-condition-analysis-and-stakeholder-decision-support

Provide Medical Care is in Critical Condition: Analysis and Stakeholder Decision Support to Minimize Further Harm

Cyber attacks lead to **1) IT network failure** and disrupt the ability of healthcare systems to access electronic health records (EHRs) and may close hospitals with IT network-based services—such as cardiac technology —and increase hospital strain (i.e., reduced capacity to take in new patients diverting critical care patients to further hospitals). **2) Ambulance diversion**, which is an important system-level interruption that causes delays in treatment and effecting time tolerance, lowering quality of care. In the long term, hospitals that experience cyber events are more likely to experience **3) hospital strain** (measured by ICU bed utilization), worsening health outcomes and contribute to **4) increased mortality**.

Figure 8 – Conceptual Model of Impact of Cyber Attack on Patient Outcomes

IST
I AM THE Cavalry

GNH
UAH
UAH
UAH
UAH

WHICH IS MORE IMPORTANT?

BRIEF REPORT

OPEN

Ransomware Cyberattack Associated With Cardiac Arrest Incidence and Outcomes at Untargeted, Adjacent Hospitals

Thaidan T. Pham, MD[1]
Theoren M. Loo, MS[2]
Atul Malhotra, MD[3]
Christopher A. Longhurst, MD, MS[4,5]
Diana Hylton, MD[6]
Christian Dameff, MD, MS[4,7,8]
Jeffrey Tully, MD[6]
Gabriel Wardi, MD, MPH[3,7]
Rebecca E. Sell, MD[9]
Alex K. Pearce, MD[3]

OBJECTIVES: Healthcare ransomware cyberattacks have been associated with major regional hospital disruptions, but data reporting patient-oriented outcomes in critical conditions such as cardiac arrest (CA) are limited. This study examined the CA incidence and outcomes of untargeted hospitals adjacent to a ransomware-infected healthcare delivery organization (HDO).

DESIGN, SETTING, AND PATIENTS: This cohort study compared the CA incidence and outcomes of two untargeted academic hospitals adjacent to an HDO under a ransomware cyberattack during the pre-attack (April 3–30, 2021), attack (May 1–28, 2021), and post-attack (May 29, 2021–June 25, 2021) phases.

INTERVENTIONS: None.

MEASUREMENTS AND MAIN RESULTS: Emergency department and hospital mean daily census, number of CAs, mean daily CA incidence per 1,000 admissions, return of spontaneous circulation, survival to discharge, and survival with favorable neurologic outcome were measured. The study evaluated 78 total CAs: 44 out-of-hospital CAs (OHCAs) and 34 in-hospital CAs. The number of total CAs increased from the pre-attack to attack phase (21 vs. 38; $p = 0.03$), followed by a decrease in the post-attack phase (38 vs. 19; $p = 0.01$). The number of total CAs exceeded the cyberattack month forecast (May 2021: 41 observed vs. 27 forecasted cases; 95% CI, 17.0–37.4). OHCA cases also exceeded the

10x DECREASE

#RSAC

SECURITY

An Illinois hospital is the first health care facility to link its closing to a ransomware attack

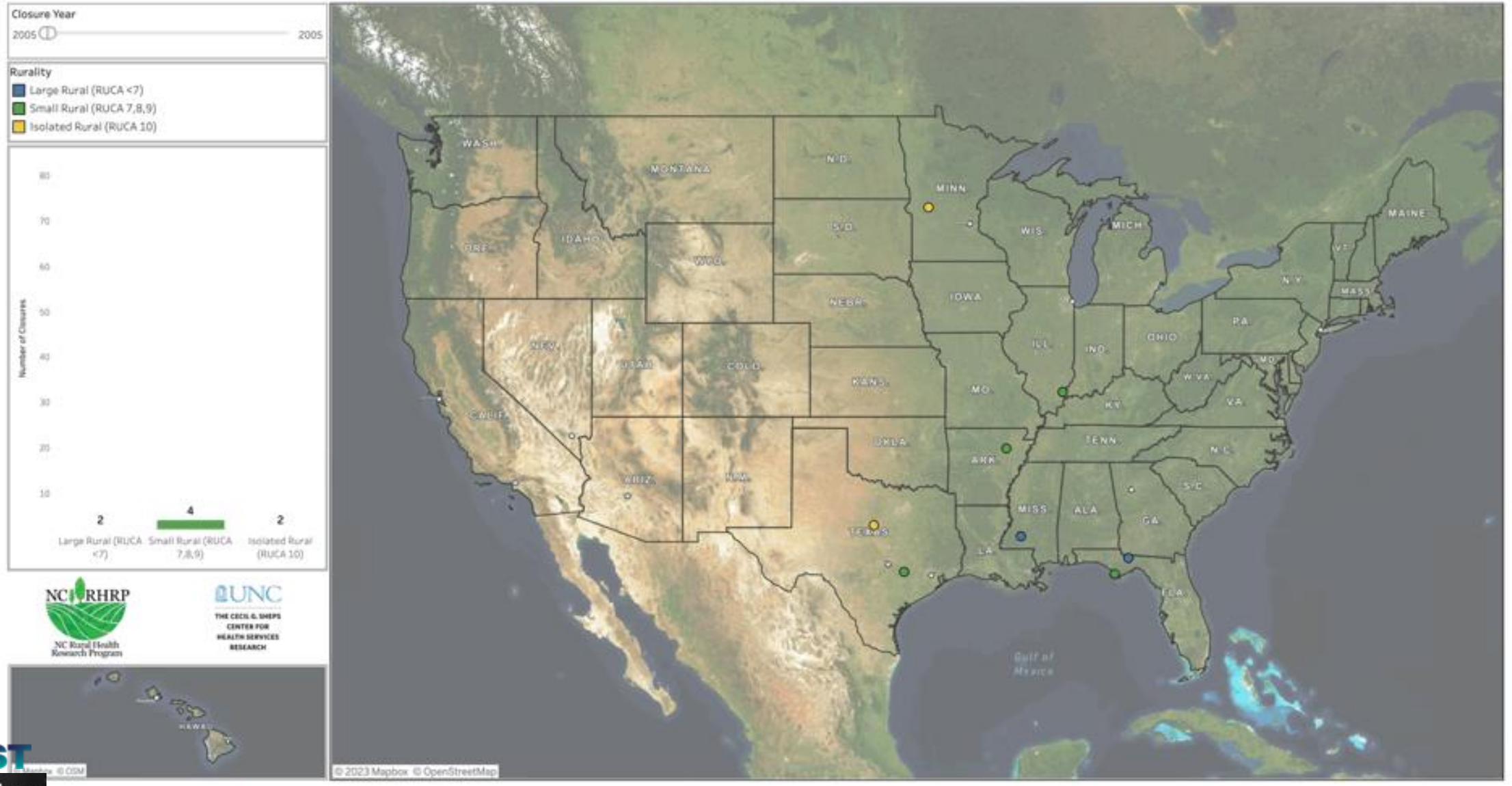
A ransomware attack hit SMP Health in 2021 and halted the hospital's ability to submit claims to insurers, Medicare or Medicaid for months, sending it into a financial spiral.

St. Margaret's Health in Spring Valley, Ill. Google Maps

IST I AM THE Cavalry

Rural Hospital Closures Maps, 2005 – Present

Closures by Era | Closures by Medicare Payment Classification | **Closures by Rurality** | Complete vs Converted Closures | Closures over time



IST
I AM THE Cavalry

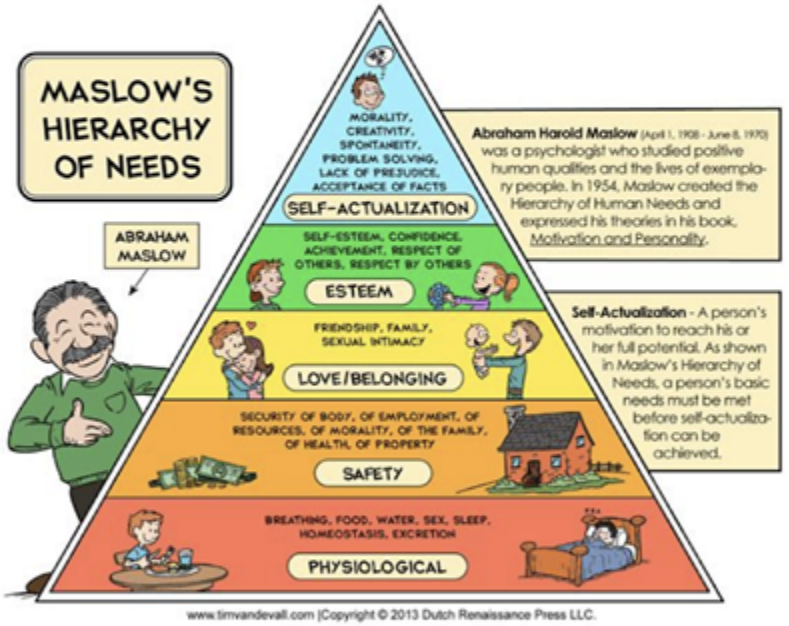
WHICH IS MORE IMPORTANT?

PROTECT SENSITIVE INFORMATION

[PHI - HIPAA]

PROVIDE MEDICAL CARE

*positions illustrative, not definitive


MASLOW'S HIERARCHY OF NEEDS
ABRAHAM MASLOW
MORALITY, CREATIVITY, SPONTANEITY, PROBLEM SOLVING, LACK OF PREJUDICE, ACCEPTANCE OF FACTS
SELF-ACTUALIZATION
SELF-ESTEEM, CONFIDENCE, ACHIEVEMENT, RESPECT OF OTHERS, RESPECT BY OTHERS
ESTEEM
FRIENDSHIP, FAMILY, SEXUAL INTIMACY
LOVE/BELONGING
SECURITY OF BODY, OF EMPLOYMENT, OF RESOURCES, OF MORALITY, OF THE FAMILY, OF HEALTH, OF PROPERTY
SAFETY
BREATHING, FOOD, WATER, SEX, SLEEP, HOMEOSTASIS, EXCRETION
PHYSIOLOGICAL
Abraham Harold Maslow (April 1, 1908 - June 8, 1970) was a psychologist who studied positive human qualities and the lives of exemplary people. In 1954, Maslow created the Hierarchy of Human Needs and expressed his theories in his book, Motivation and Personality.
Self-Actualization - A person's motivation to reach his or her full potential. As shown in Maslow's Hierarchy of Needs, a person's basic needs must be met before self-actualization can be achieved.
www.timvandevall.com |Copyright © 2013 Dutch Renaissance Press LLC.

Latency-*insensitive* — *months*

weeks

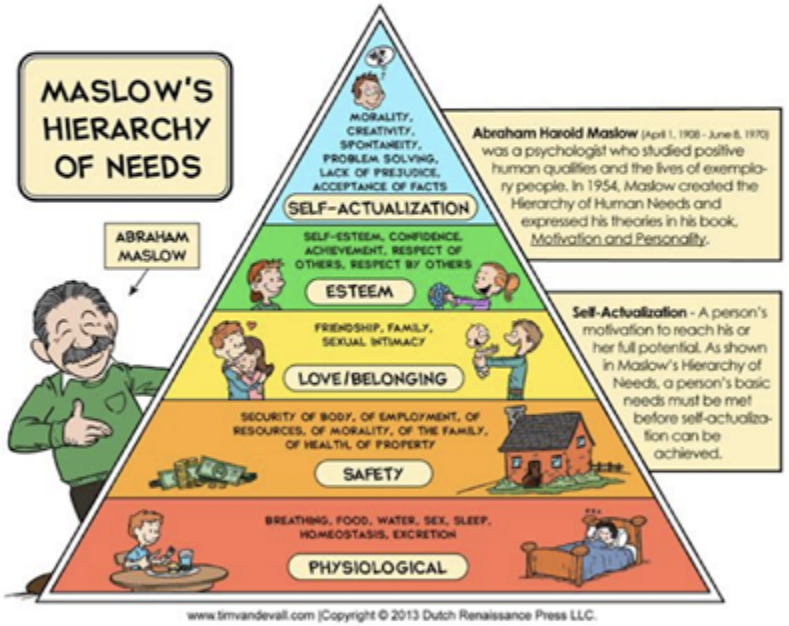
Latency-*sensitive* — *days*

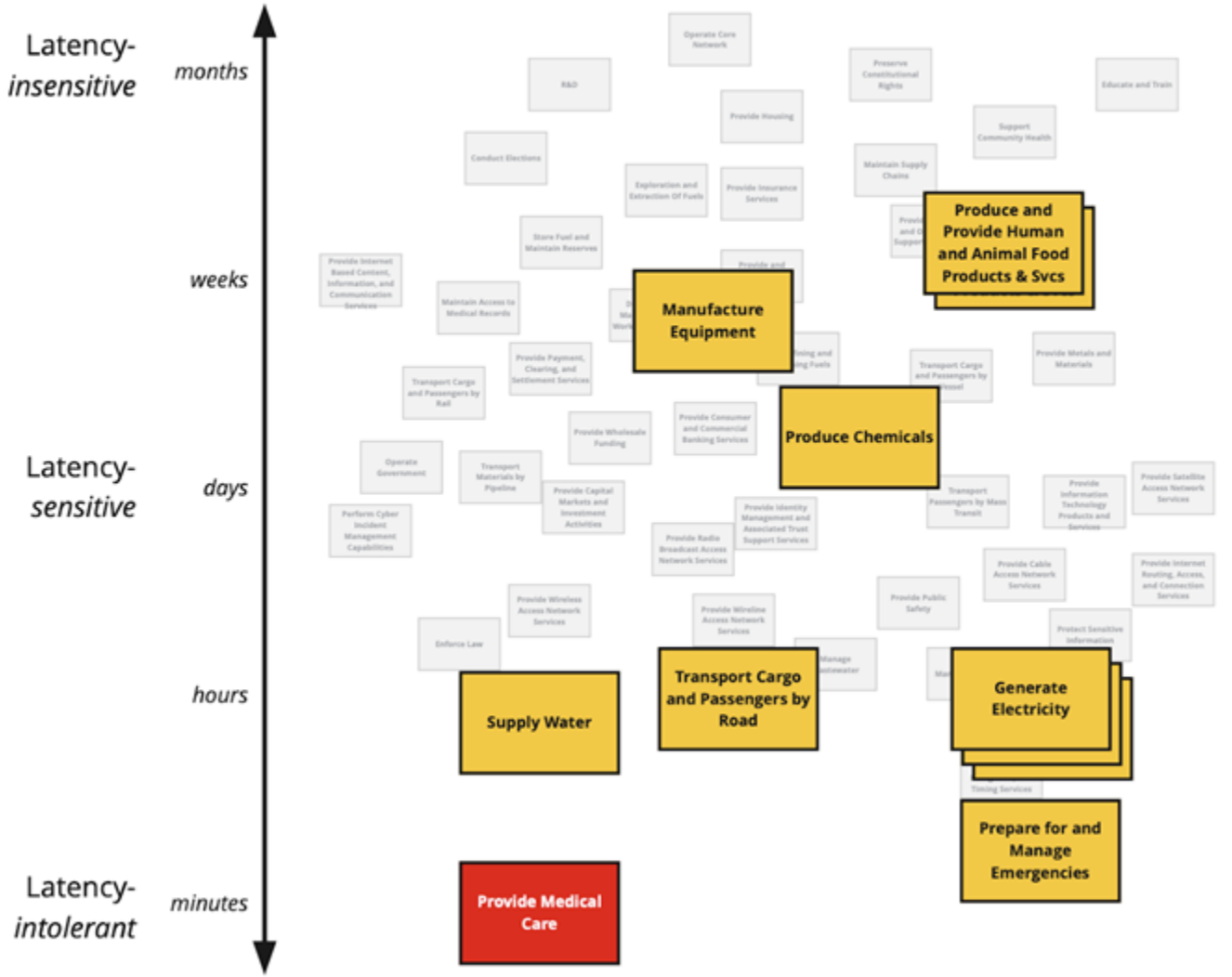
hours

Latency-*intolerant* — *minutes*

IMG SRC: Ben Mosier & Josh Corman 2022

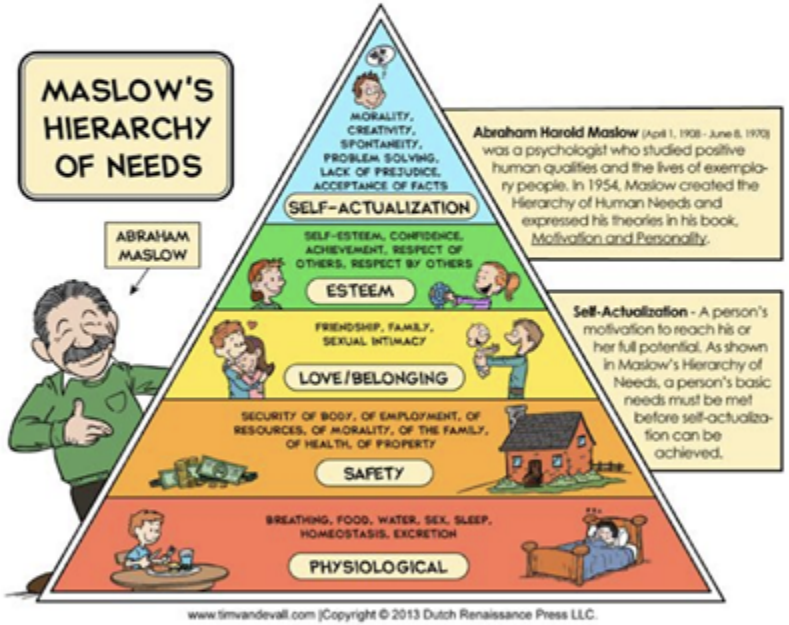
*positions illustrative, not definitive

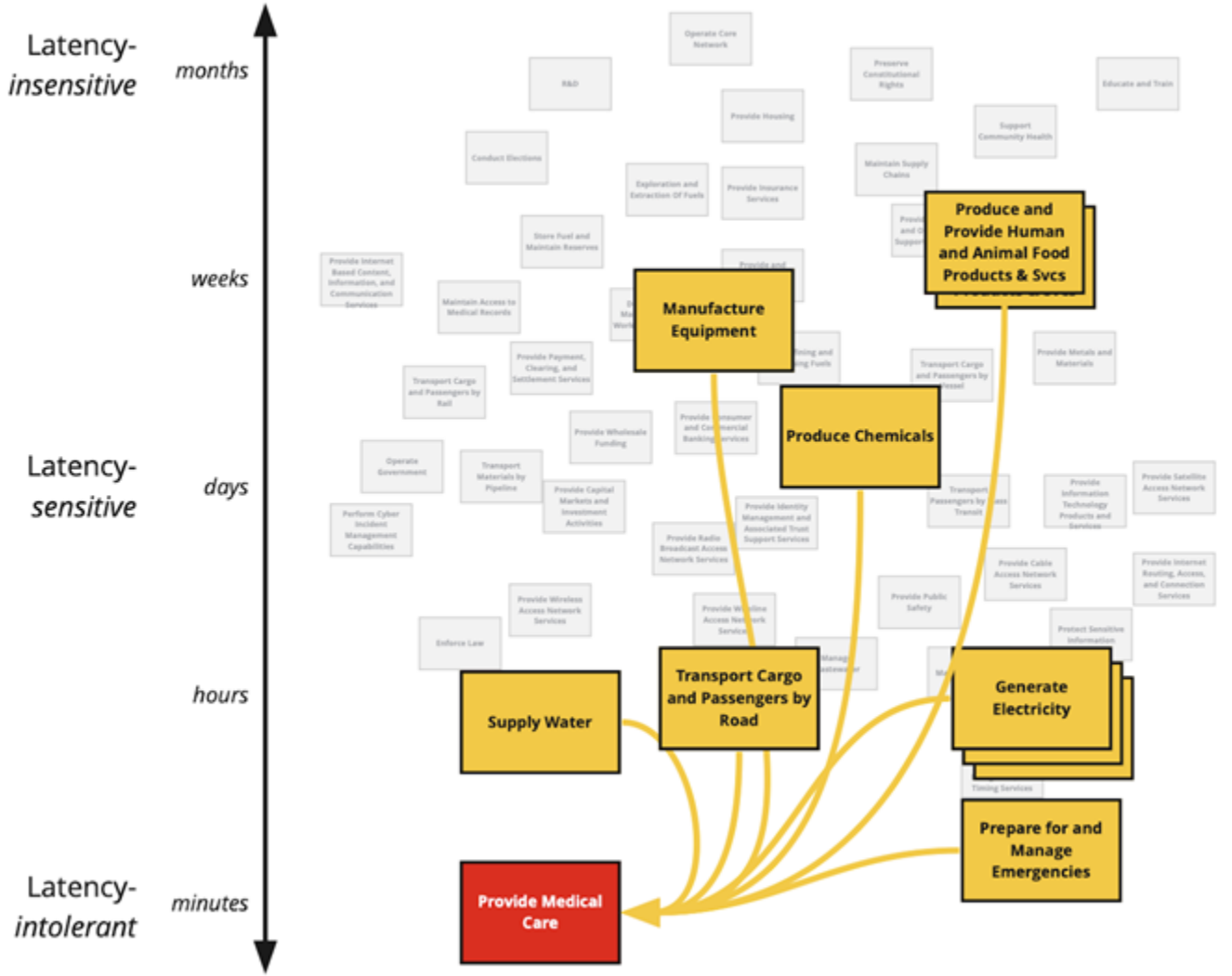

MASLOW'S HIERARCHY OF NEEDS
ABRAHAM MASLOW
MORALITY, CREATIVITY, SPONTANEITY, PROBLEM SOLVING, LACK OF PREJUDICE, ACCEPTANCE OF FACTS
SELF-ACTUALIZATION
SELF-ESTEEM, CONFIDENCE, ACHIEVEMENT, RESPECT OF OTHERS, RESPECT BY OTHERS
ESTEEM
FRIENDSHIP, FAMILY, SEXUAL INTIMACY
LOVE/BELONGING
SECURITY OF BODY, OF EMPLOYMENT, OF RESOURCES, OF MORALITY, OF THE FAMILY, OF HEALTH, OF PROPERTY
SAFETY
BREATHING, FOOD, WATER, SEX, SLEEP, HOMEOSTASIS, EXCRETION
PHYSIOLOGICAL
Abraham Harold Maslow (April 1, 1908 - June 8, 1970) was a psychologist who studied positive human qualities and the lives of exemplary people. In 1954, Maslow created the Hierarchy of Human Needs and expressed his theories in his book, Motivation and Personality.
Self-Actualization - A person's motivation to reach his or her full potential. As shown in Maslow's Hierarchy of Needs, a person's basic needs must be met before self-actualization can be achieved.
www.timvandevall.com |Copyright © 2013 Dutch Renaissance Press LLC.



IMG SRC: Ben Mosier & Josh Corman 2022

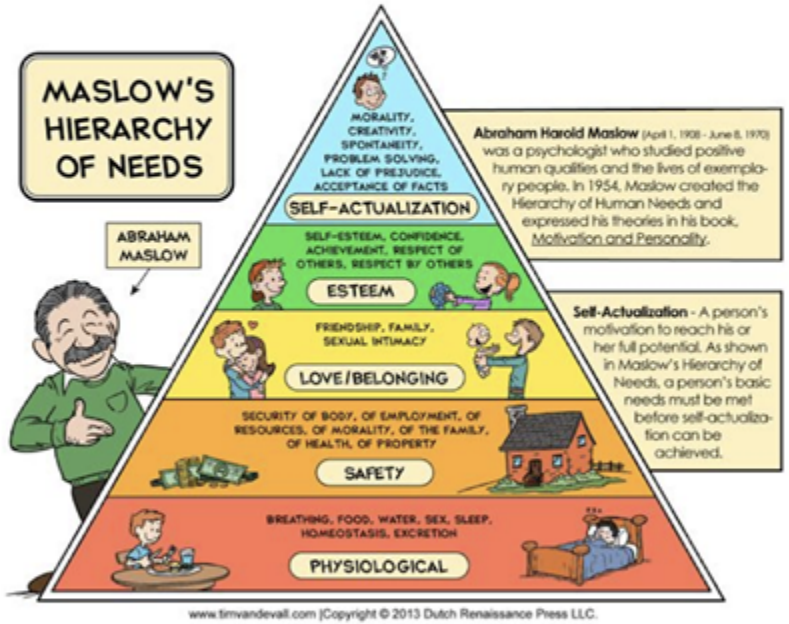
*positions illustrative, not definitive

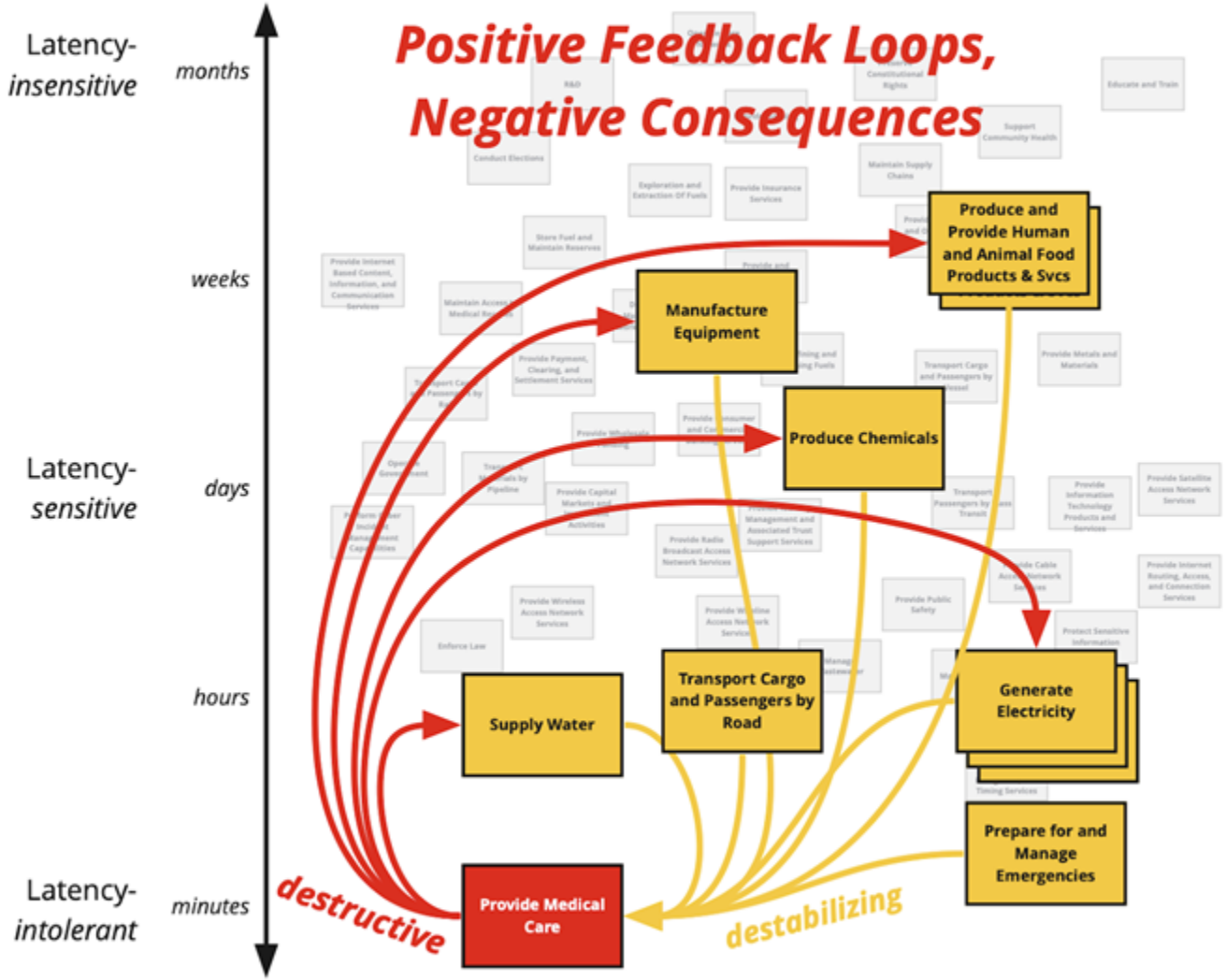

MASLOW'S HIERARCHY OF NEEDS
ABRAHAM MASLOW
MORALITY, CREATIVITY, SPONTANEITY, PROBLEM SOLVING, LACK OF PREJUDICE, ACCEPTANCE OF FACTS
SELF-ACTUALIZATION
SELF-ESTEEM, CONFIDENCE, ACHIEVEMENT, RESPECT OF OTHERS, RESPECT BY OTHERS
ESTEEM
FRIENDSHIP, FAMILY, SEXUAL INTIMACY
LOVE/BELONGING
SECURITY OF BODY, OF EMPLOYMENT, OF RESOURCES, OF MORALITY, OF THE FAMILY, OF HEALTH, OF PROPERTY
SAFETY
BREATHING, FOOD, WATER, SEX, SLEEP, HOMEOSTASIS, EXCRETION
PHYSIOLOGICAL
Abraham Harold Maslow (April 1, 1908 - June 8, 1970) was a psychologist who studied positive human qualities and the lives of exemplary people. In 1954, Maslow created the Hierarchy of Human Needs and expressed his theories in his book, Motivation and Personality.
Self-Actualization - A person's motivation to reach his or her full potential. As shown in Maslow's Hierarchy of Needs, a person's basic needs must be met before self-actualization can be achieved.
www.timvandevall.com |Copyright © 2013 Dutch Renaissance Press LLC.



IMG SRC: Ben Mosier & Josh Corman 2022

*positions illustrative, not definitive


MASLOW'S HIERARCHY OF NEEDS
ABRAHAM MASLOW
MORALITY, CREATIVITY, SPONTANEITY, PROBLEM SOLVING, LACK OF PREJUDICE, ACCEPTANCE OF FACTS
SELF-ACTUALIZATION
SELF-ESTEEM, CONFIDENCE, ACHIEVEMENT, RESPECT OF OTHERS, RESPECT BY OTHERS
ESTEEM
FRIENDSHIP, FAMILY, SEXUAL INTIMACY
LOVE/BELONGING
SECURITY OF BODY, OF EMPLOYMENT, OF RESOURCES, OF MORALITY, OF THE FAMILY, OF HEALTH, OF PROPERTY
SAFETY
BREATHING, FOOD, WATER, SEX, SLEEP, HOMEOSTASIS, EXCRETION
PHYSIOLOGICAL
Abraham Harold Maslow (April 1, 1908 - June 8, 1970) was a psychologist who studied positive human qualities and the lives of exemplary people. In 1954, Maslow created the Hierarchy of Human Needs and expressed his theories in his book, Motivation and Personality.
Self-Actualization - A person's motivation to reach his or her full potential. As shown in Maslow's Hierarchy of Needs, a person's basic needs must be met before self-actualization can be achieved.
www.timvandevall.com |Copyright © 2013 Dutch Renaissance Press LLC.



IMG SRC: Ben Mosier & Josh Corman 2022

IST Institute for SECURITY + TECHNOLOGY

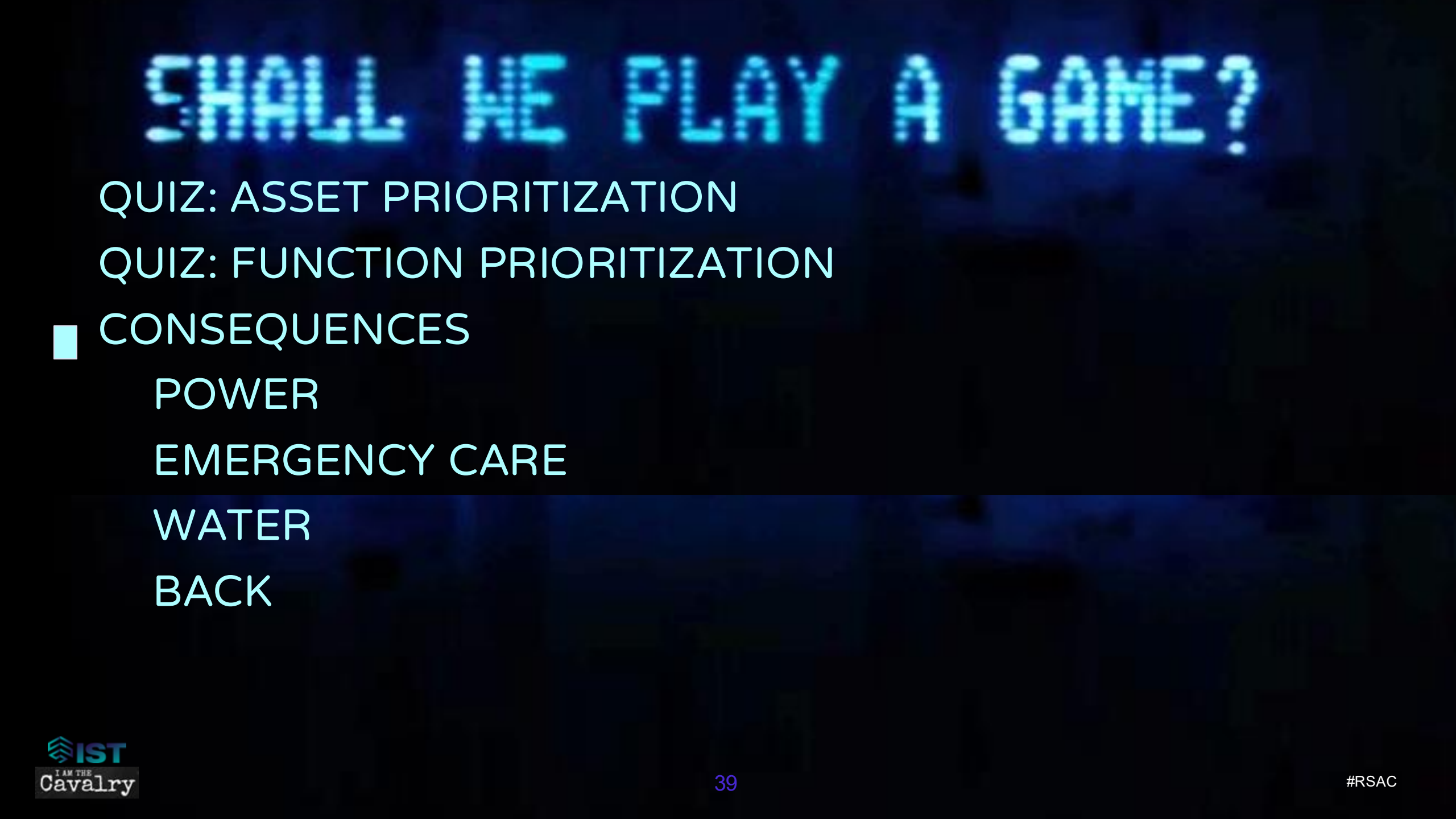
DONATE EXPLORE

IST I AM THE Cavalry

UnDisruptable27.org

SHALL WE PLAY A GAME?

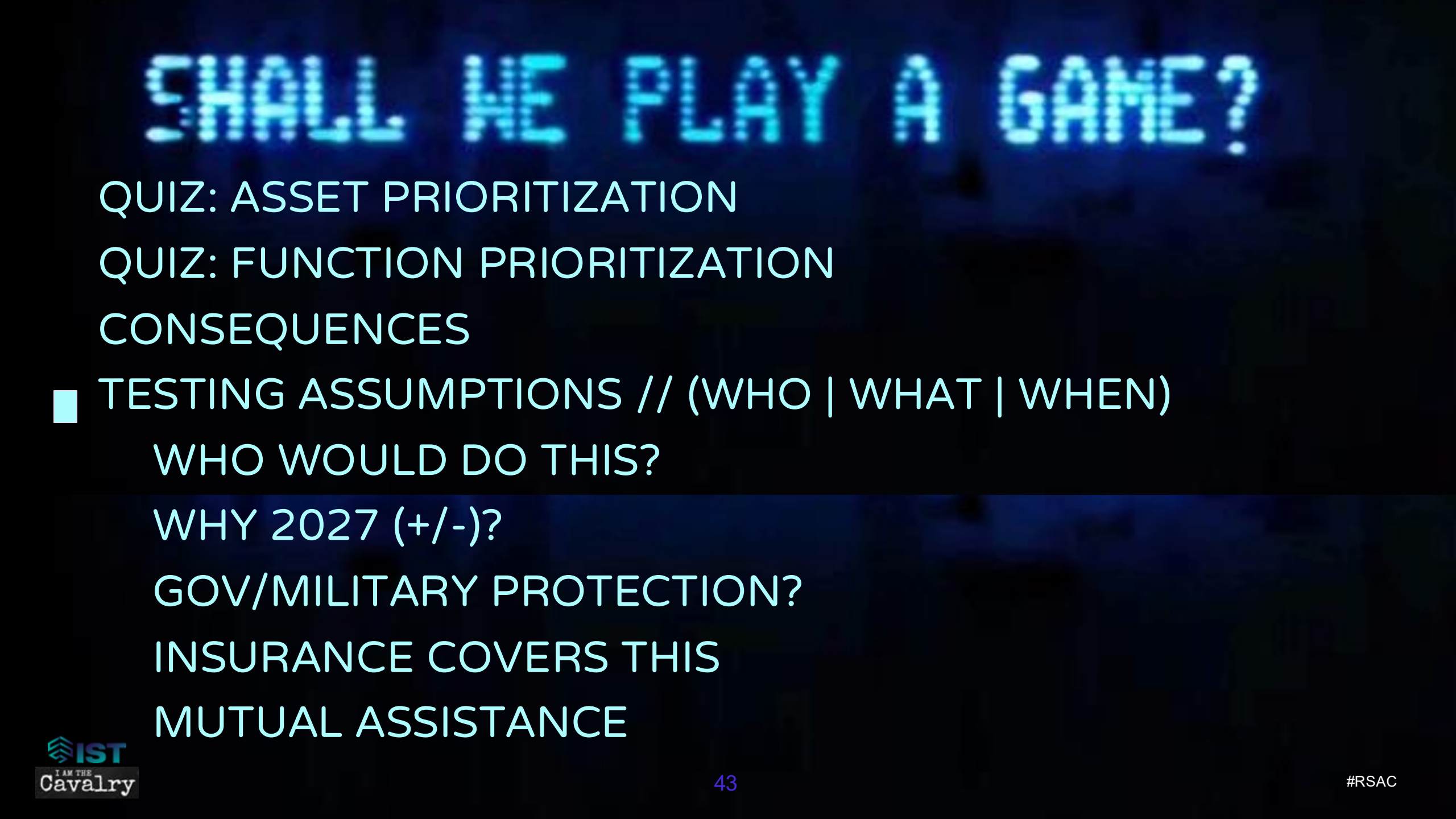
- QUIZ: ASSET PRIORITIZATION
- QUIZ: FUNCTION PRIORITIZATION
- CONSEQUENCES
- TESTING ASSUMPTIONS // (WHO | WHAT | WHEN)
- HAMMER TIME // VOLT TYPHOON SIMULATION
- THE BEST DEFENSE…
- PRIORITIZATION: RELOADED
- RETURN HOME



- QUIZ: ASSET PRIORITIZATION
- QUIZ: FUNCTION PRIORITIZATION
- CONSEQUENCES
  - POWER
  - EMERGENCY CARE
  - WATER
  - BACK

CONSEQUENCES... ...?

CONSEQUENCES... ...?



- QUIZ: ASSET PRIORITIZATION
- QUIZ: FUNCTION PRIORITIZATION
- CONSEQUENCES
- TESTING ASSUMPTIONS // (WHO | WHAT | WHEN)
  - WHO WOULD DO THIS?
  - WHY 2027 (+/-)?
  - GOV/MILITARY PROTECTION?
  - INSURANCE COVERS THIS
  - MUTUAL ASSISTANCE

BUT WHO WOULD DO THIS...?

CHINA (2027)

IRAN (SOONER?)

RUSSIA

DPRK?

WHY 2027 (+/-) ... ...

TLP:CLEAR
PRC STATE-SPONSORED CYBER ACTIVITY: ACTIONS FOR CRITICAL INFRASTRUCTURE LEADERS
ASD
ACSC
National Cyber Security Centre
a part of GCHQ

VOLT TYPHOON

Jan 31, 2024, 10:55:13 AM
Select Committee on the Chinese Communist Party
Room 390
The CCP Cyber Threat to the American Homeland and National Security
The Select Committee on the CCP
Subscribe

GOV/MILITARY PROTECTION ...?

85% CRITICAL INFRASTRUCTURE IS PRIVATE

NO DOMESTIC DEFENSIVE “CYBER FORCE”

EXECUTIVE ORDER 14239 —>

MS-ISAC?

SRMAs? and CIPAC?

CISA?

CONGRESS?

...

whitehouse.gov/presidential-actions/2025/03/test/
PRESIDENT DONALD J. TRUMP
The WHITE HOUSE
PRESIDENTIAL ACTIONS
Achieving Efficiency Through State and Local Preparedness
The White House | March 19, 2025
By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered:
Section 1. Purpose. Commonsense approaches and investments by State and local governments across American infrastructure will enhance national security and create a more resilient Nation. Federal policy must rightly recognize that preparedness is most effectively owned and managed at the State, local, and even individual levels, supported by a competent, accessible, and efficient Federal Government. Citizens are the immediate beneficiaries of sound local decisions and investments designed to address risks, including cyber attacks,

INSURANCE ... ...?

EXCLUSIONS: “ACTS OF WAR”

EXCLUSIONS: INFRASTRUCTURE OUTAGE

CYBERACUVIEW*

CYBER-LIFELINE BACKSTOP?

*Cyber Insurance Consortium with 20+ Member (60% of US Cyber Insurance Market)

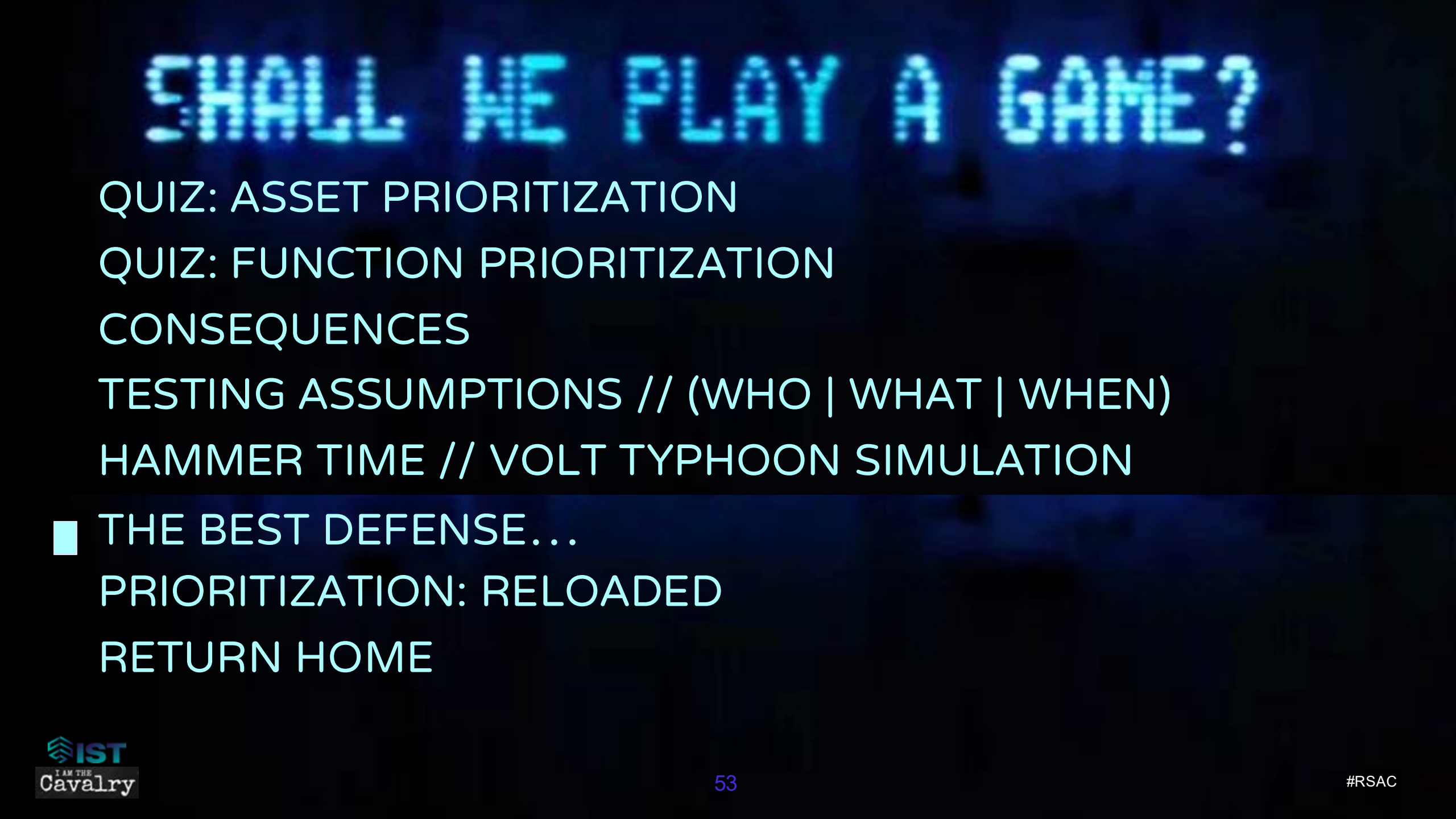
FALLACY: MUTUAL ASSISTANCE

SHALL WE PLAY A GAME?

- QUIZ: ASSET PRIORITIZATION
- QUIZ: FUNCTION PRIORITIZATION
- CONSEQUENCES
- TESTING ASSUMPTIONS // (WHO | WHAT | WHEN)
- HAMMER TIME // VOLT TYPHOON SIMULATION
- THE BEST DEFENSE…
- PRIORITIZATION: RELOADED
- RETURN HOME

HAMMER TIME!!! ...?

HAMMER TIME!!! ...?

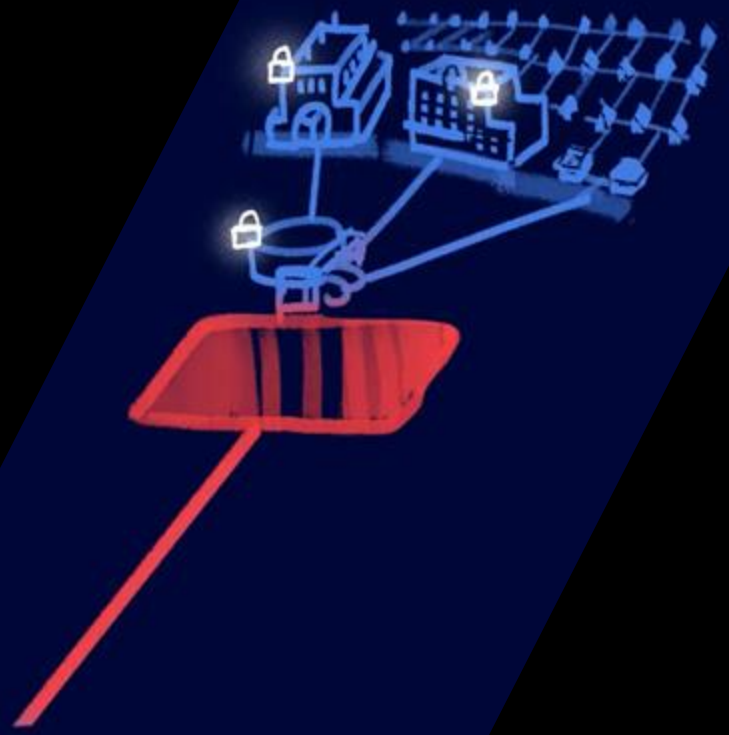


- QUIZ: ASSET PRIORITIZATION
- QUIZ: FUNCTION PRIORITIZATION
- CONSEQUENCES
- TESTING ASSUMPTIONS // (WHO | WHAT | WHEN)
- HAMMER TIME // VOLT TYPHOON SIMULATION
- THE BEST DEFENSE…
- PRIORITIZATION: RELOADED
- RETURN HOME

THE BEST DEFENSE...?

SHIELDS

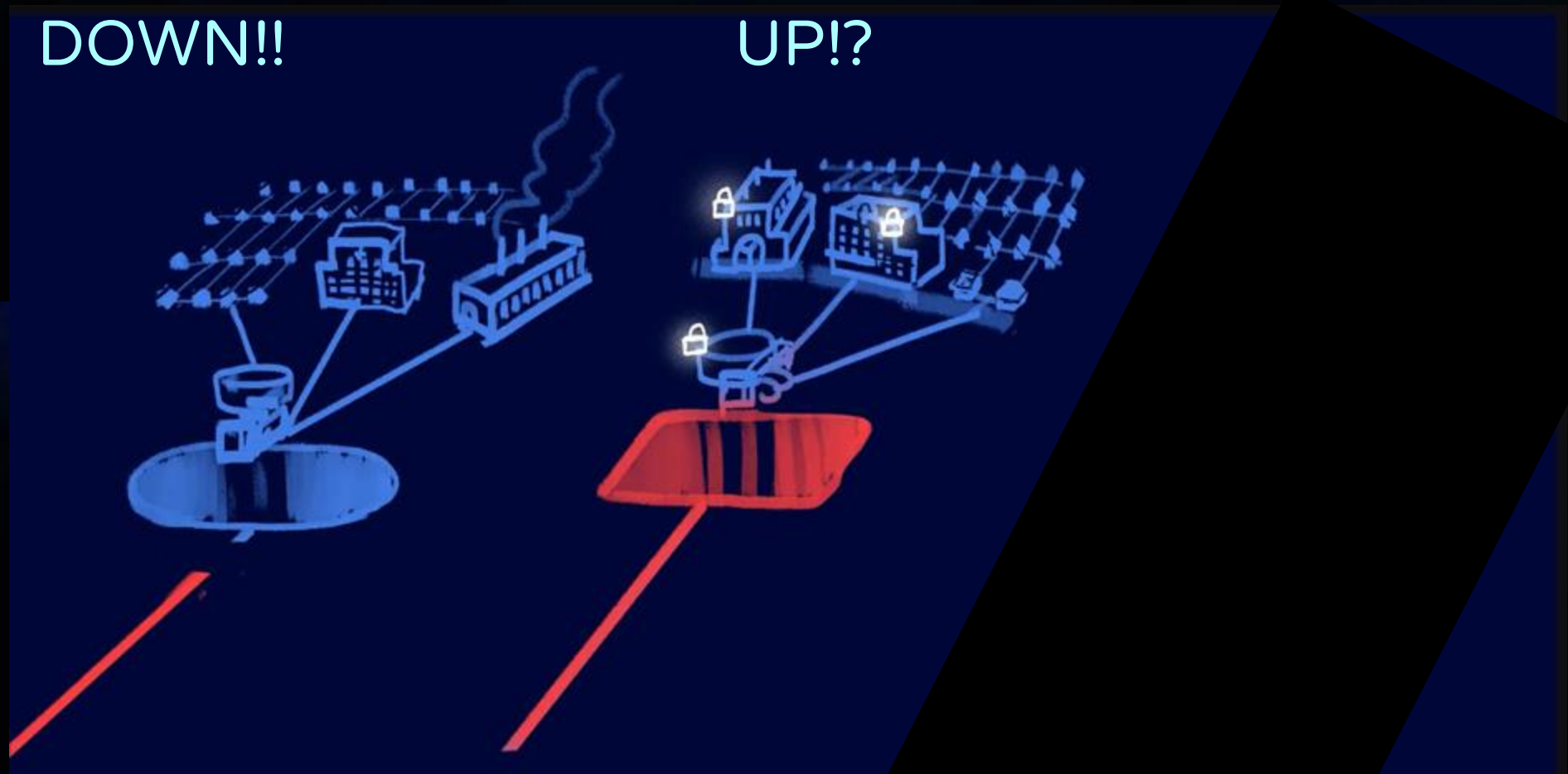
UP!?



THE BEST DEFENSE...?

CONNECTIONS DOWN!!

SHIELDS UP!?



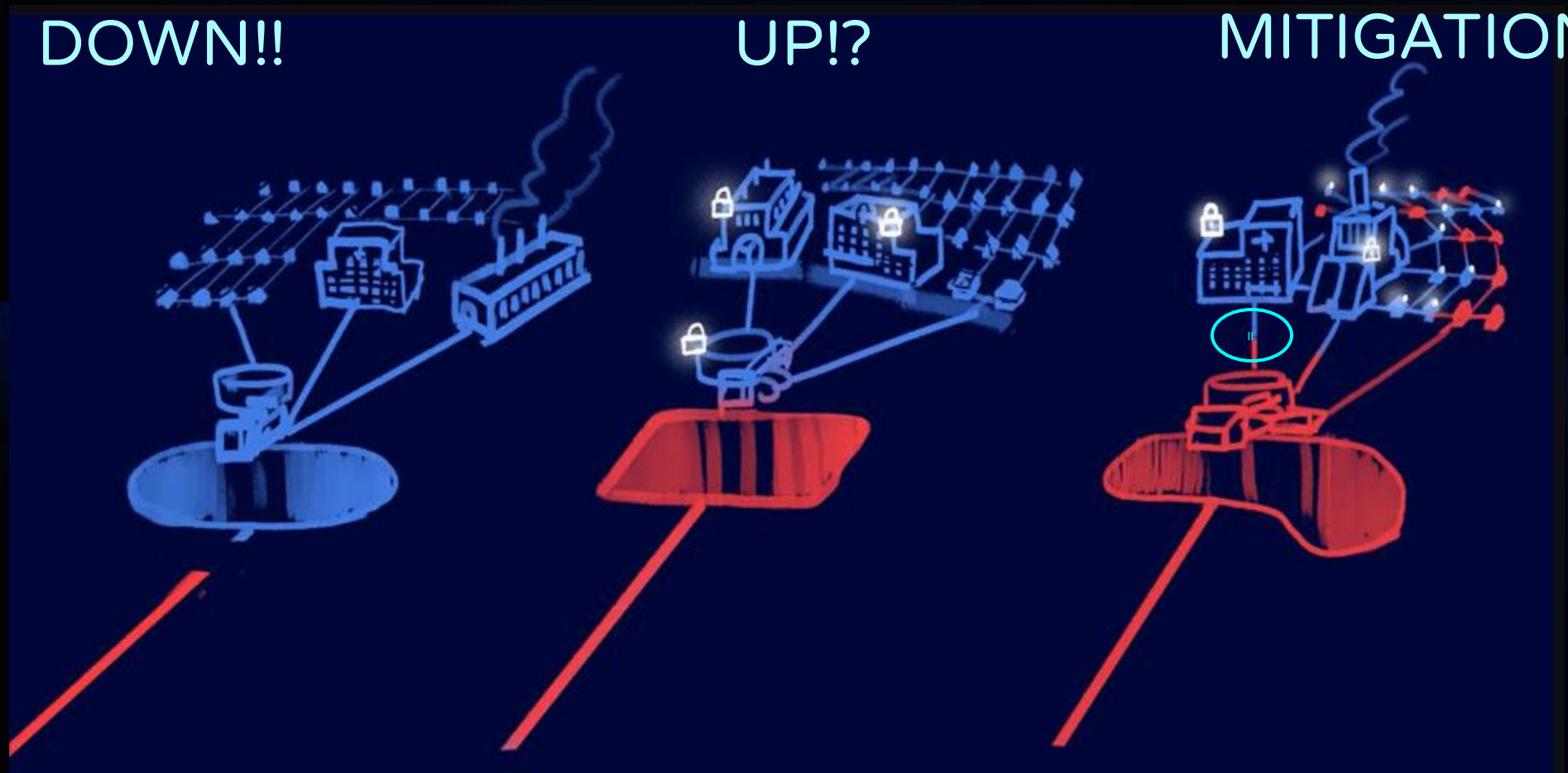
IST I AM THE Cavalry

THE BEST DEFENSE...?

CONNECTIONS DOWN!!

SHIELDS UP!?

PHYSICAL MITIGATIONS



IST I AM THE Cavalry

INL CIE > HAMMER TIME!!!

INL CIE > HAMMER TIME!!!

What Is Risk?

RISK = PROBABILITY / LIKELIHOOD / CREDIBILITY × IMPACT / CONSEQUENCE

ENGINEERING

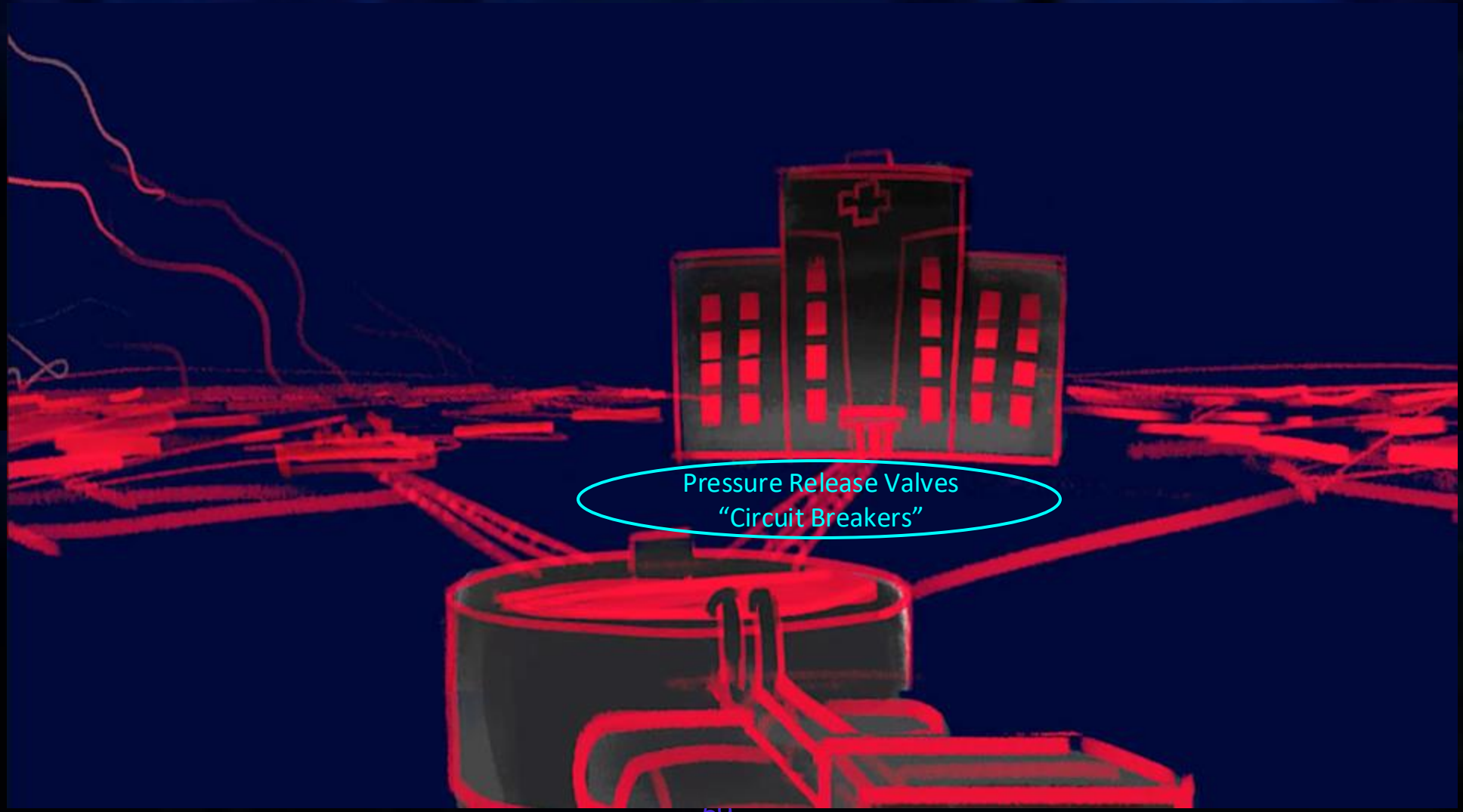
2

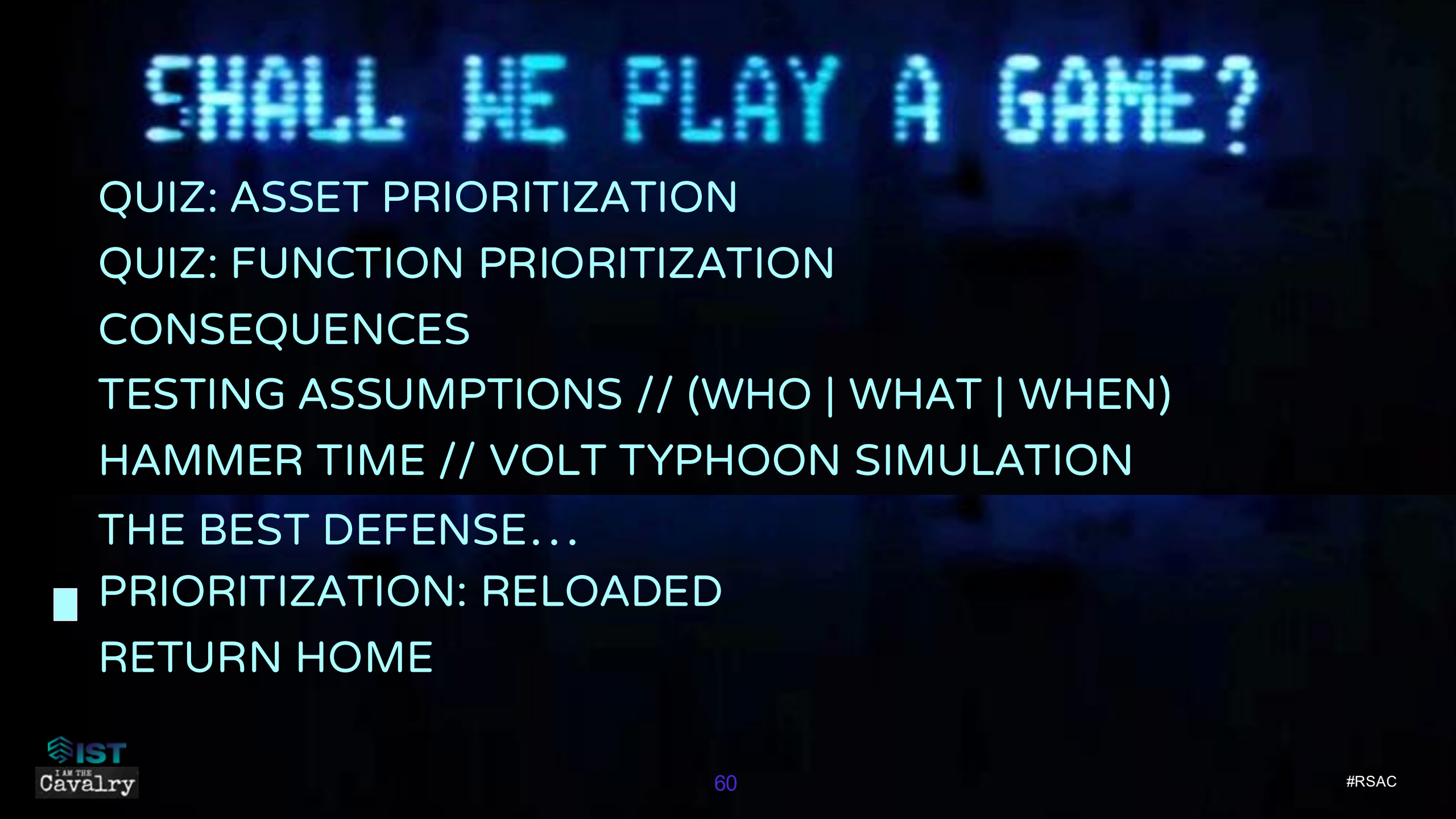
Sponsored by DOE CESER and performed by Idaho National Laboratory and the National Renewable Energy Laboratory

Cyber-Informed Engineering

IST I AM THE Cavalry

THE BEST DEFENSE...?





- QUIZ: ASSET PRIORITIZATION
- QUIZ: FUNCTION PRIORITIZATION
- CONSEQUENCES
- TESTING ASSUMPTIONS // (WHO | WHAT | WHEN)
- HAMMER TIME // VOLT TYPHOON SIMULATION
- THE BEST DEFENSE…
- PRIORITIZATION: RELOADED
- RETURN HOME

WHICH IS MORE IMPORTANT?

PROVIDE WATER

PROVIDE MEDICAL CARE

WHICH IS MORE IMPORTANT?

PROVIDE WATER TO DIALYSIS CENTER

PROVIDE WATER TO TRAUMA CENTER

WHICH IS MORE IMPORTANT?

PROVIDE WATER TO
1of1 HOSPITALS

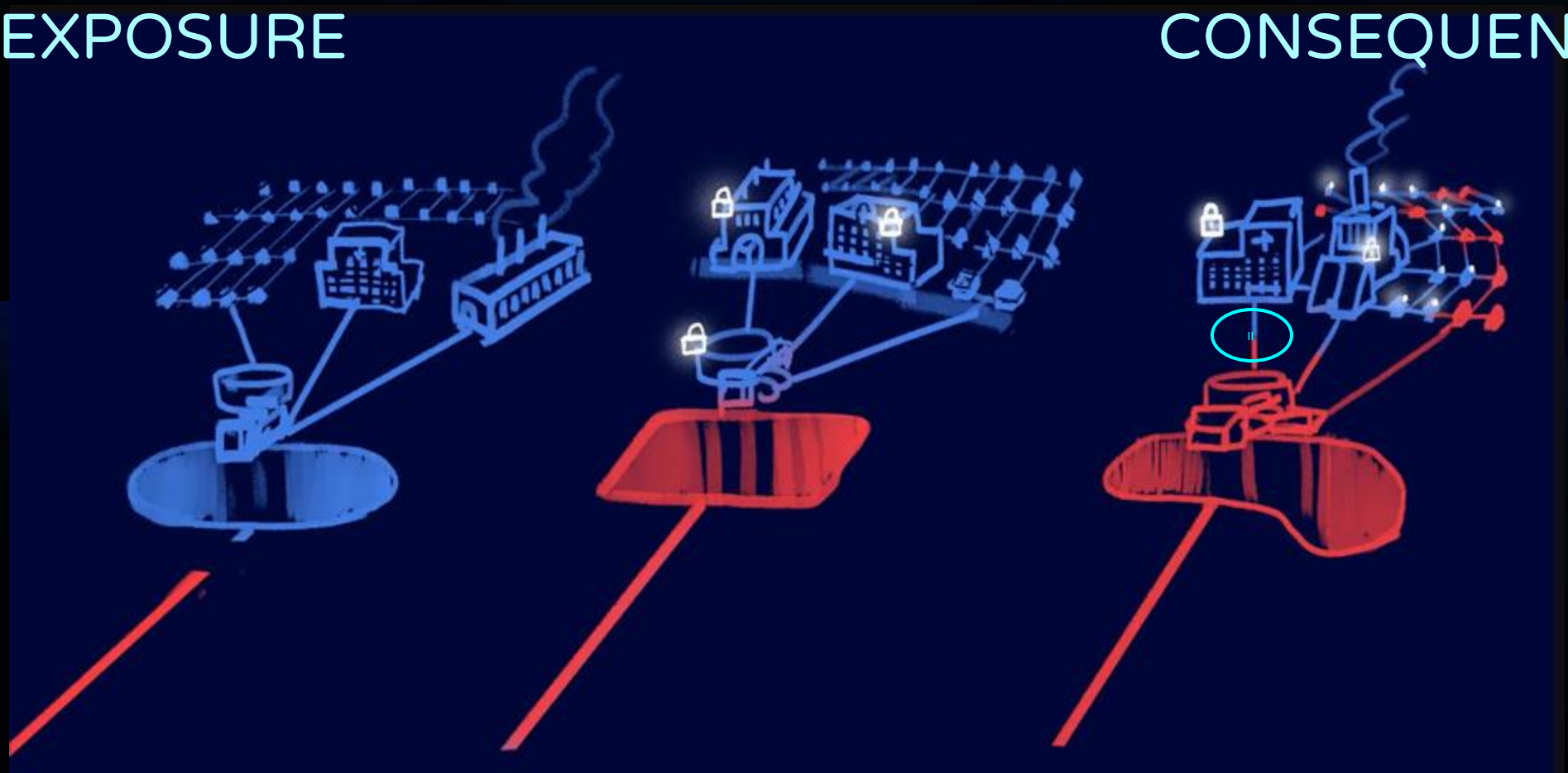
PROVIDE WATER TO
1of3 HOSPITALS

WHICH IS MORE IMPORTANT?

REMOVE EXPOSURE

ADD CYBER?

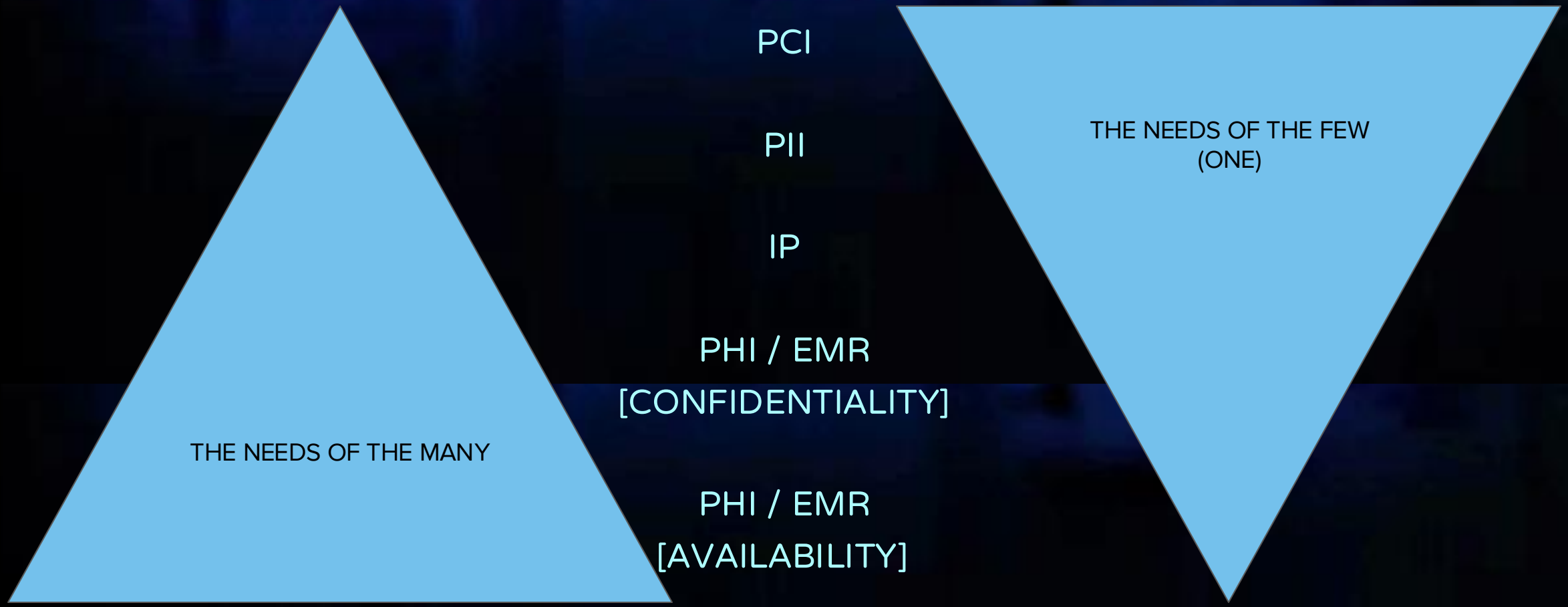
ENGINEER DOWN CONSEQUENCES



IST
I AM THE Cavalry

REPRISE: WHY?

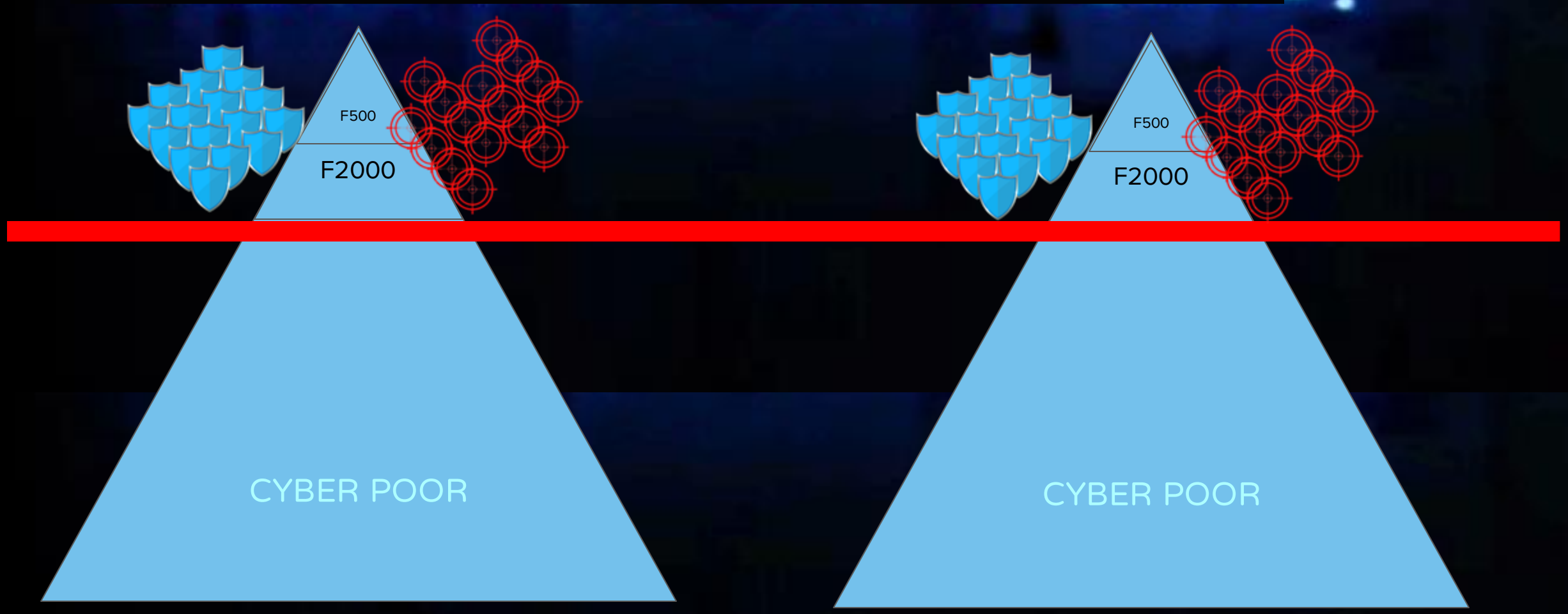
WHICH IS MORE IMPORTANT?



MASLOW'S

CYBERSECURITY

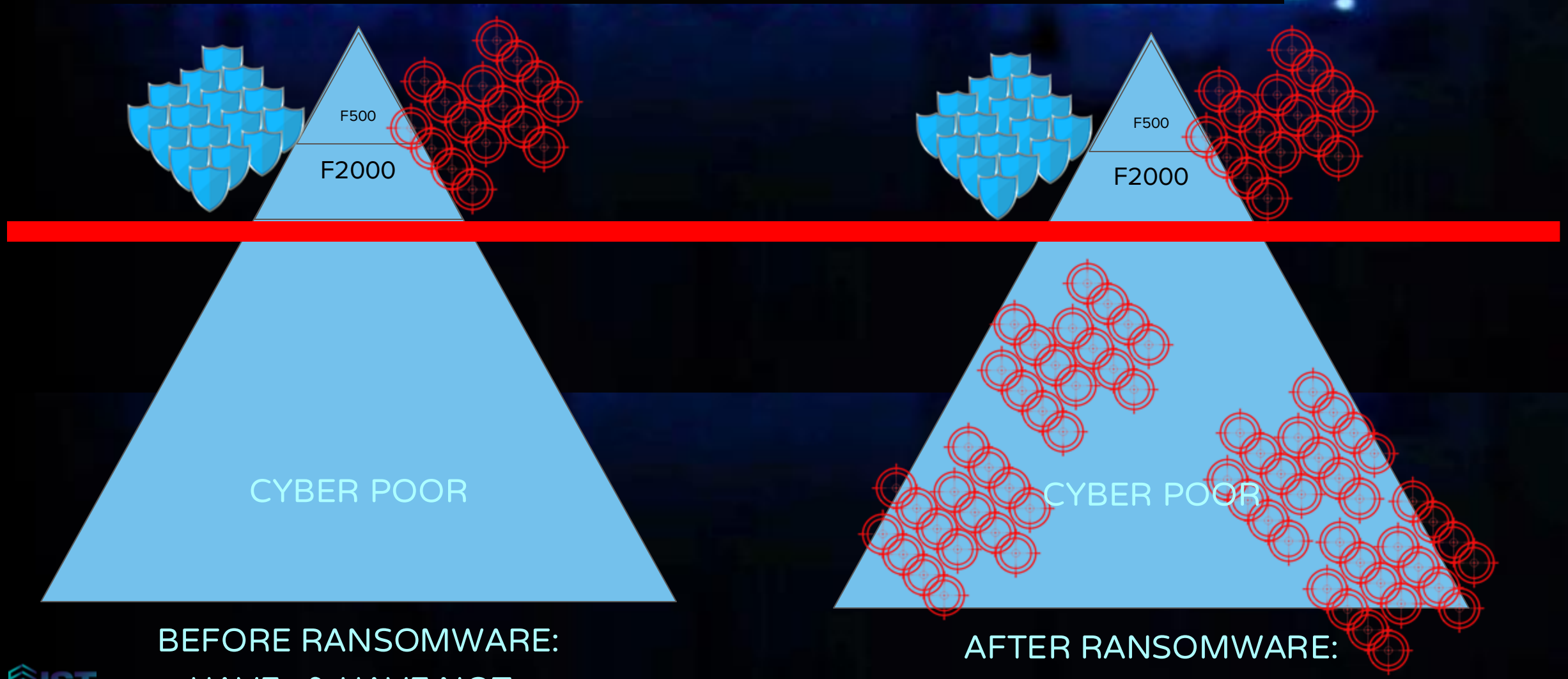
REPRISE: WHY?
WHICH IS MORE IMPORTANT?



BEFORE RANSOMWARE:
HAVEs & HAVE NOTs

AFTER RANSOMWARE:
HAVEs & HAVE NOTs

REPRISE: WHY?
WHICH IS MORE IMPORTANT?



BEFORE RANSOMWARE:
HAVEs & HAVE NOTs

AFTER RANSOMWARE:
HAVEs & HAVE NOTs

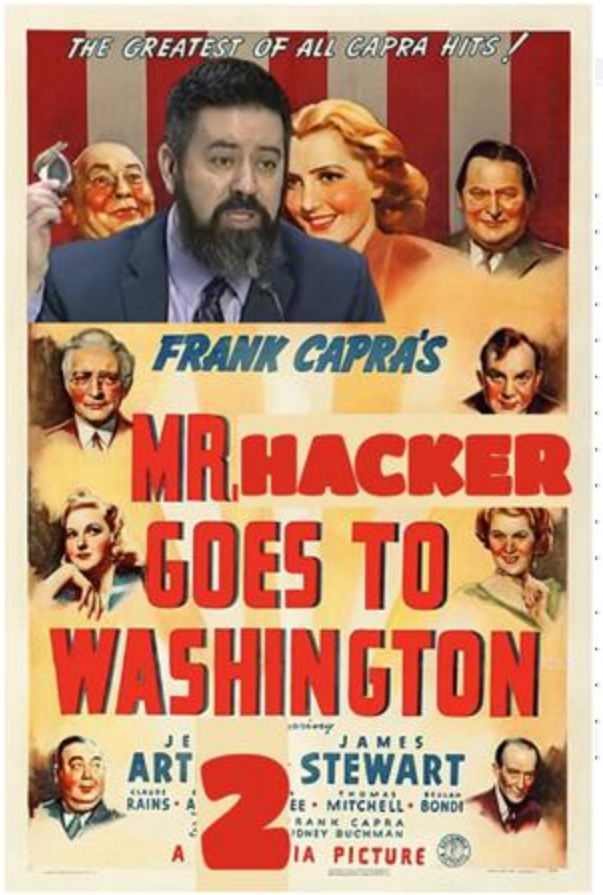
Target Rich; Cyber Poor

Information
Incentives
Resources

iamthecavalry.org

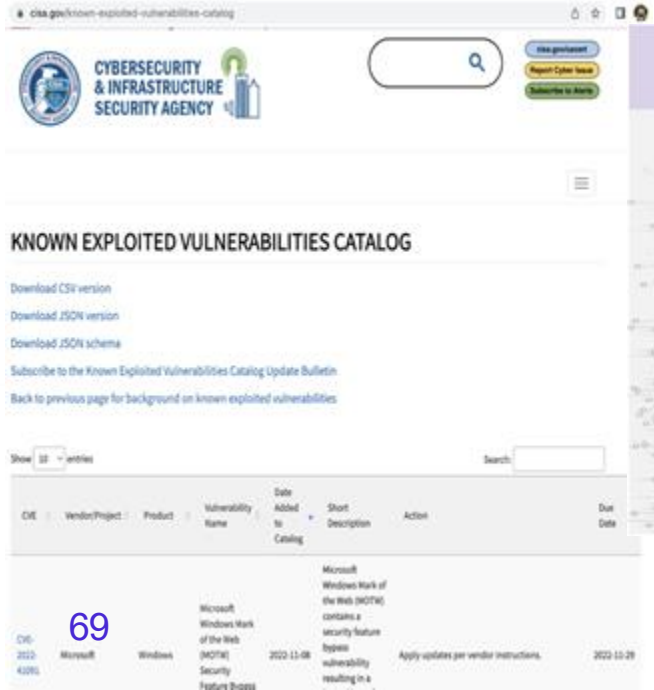
I AM THE Cavalry

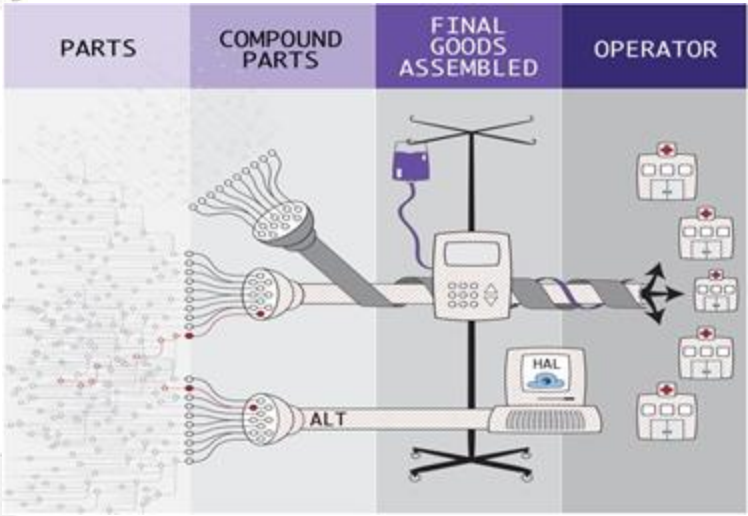
CISA COVID Task Force



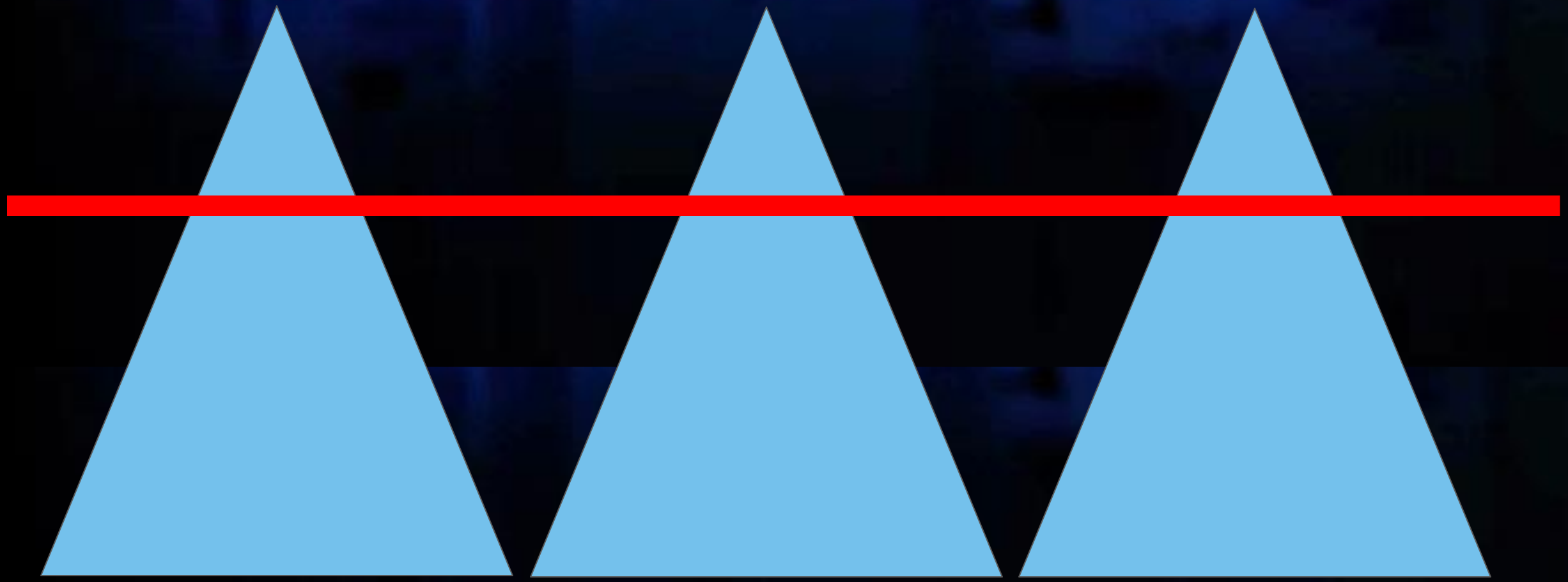
BAD PRACTICES
BAD PRACTICES
As recent incidents have demonstrated, cyberattacks against critical infrastructure can have significant impacts on the critical functions of government and the private sector. All organizations, and particularly those supporting designated Critical Infrastructure or National Critical Functions (NCF)[1] should implement an effective cybersecurity program to protect against cyber threats and manage cyber risk in a manner commensurate with the criticality of those NCFs to national security, national economic security, and/or national public health and safety.
CISA is developing a catalog of Bad Practices that are exceptionally risky, especially in organizations supporting Critical Infrastructure or NCFs. The presence of these Bad Practices in organizations that support Critical Infrastructure or NCFs is exceptionally dangerous and increases risk to our critical infrastructure, on which we rely for national security, economic stability, and life, health, and safety of the public. Entries in the catalog will be listed here as they are added.
1. Use of unsupported (or end-of-life) software in service of Critical Infrastructure and National Critical Functions is dangerous and significantly elevates risk to national security, national economic security, and national public health and safety. This dangerous practice is especially egregious in technologies accessible from the Internet.
2. Use of known/fixed/default passwords and credentials in service of Critical Infrastructure and National Critical Functions is dangerous and significantly elevates risk to national security, national economic security, and national public health and safety. This dangerous practice is especially egregious in technologies accessible from the Internet.
3. The use of single-factor authentication for remote or administrative access to systems supporting the operation of Critical Infrastructure and National Critical Functions (NCF) is dangerous and significantly elevates risk to national security, national economic security, and national public health and safety. This dangerous practice is especially egregious in technologies accessible from the Internet.
While these practices are dangerous for Critical Infrastructure and NCFs, CISA encourages all organizations to engage in the necessary actions and critical conversations to address Bad Practices."

Critical Infrastructure S.O.S.
Get your Stuff Off Search.
KNOW WHAT YOUR ADVERSARIES KNOW!
Attackers are increasingly working to compromise cyber and physical security –
Don't get caught off guard – Get your Stuff Off Search – S.O.S.!
While zero-day attacks draw the most attention, frequently less-complex exposures to both cyber and physical security are missed. Get your Stuff Off Search – S.O.S. – and reduce Internet attack surfaces that are visible to anyone on web-based search platforms.
Exposures increasingly include Industrial Internet of Things (IIoT), Supervisory Control and Data Acquisition systems (SCADA), industrial control systems (ICS), remote access technologies, and other critical assets – which may impact public safety, human life, and national security. CISA can help you:
#1 ASSESS YOUR POSTURE
You have probably done a lot to secure your facilities. However, without visibility into your assets that are accessible across the Internet, you may not fully understand your potential for being attacked. While many people use search engines to find cat pictures, cyber attackers commonly use similar tools to locate Internet-connected IIoT devices. In fact, once a device is identified, hacking is not even required in many cases – for example, if





WHICH IS MORE IMPORTANT?

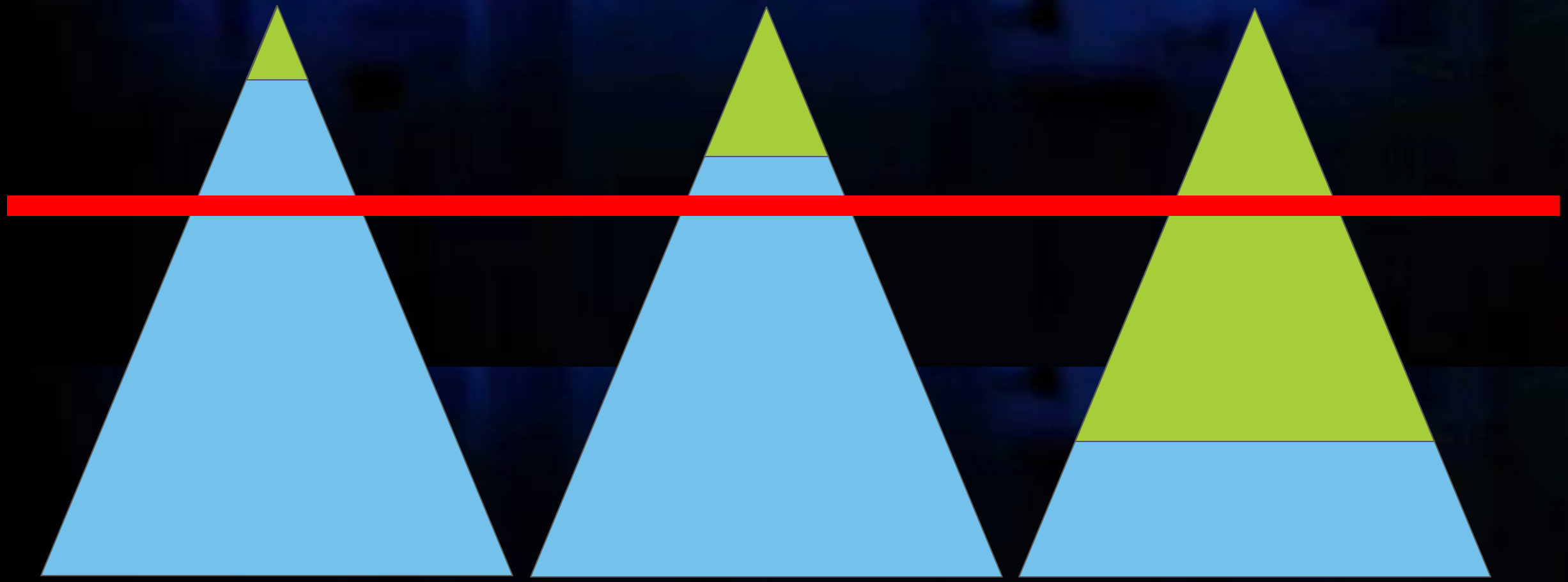


WATER

EMERGENCY CARE

ENERGY/POWER

WHICH IS MORE IMPORTANT?

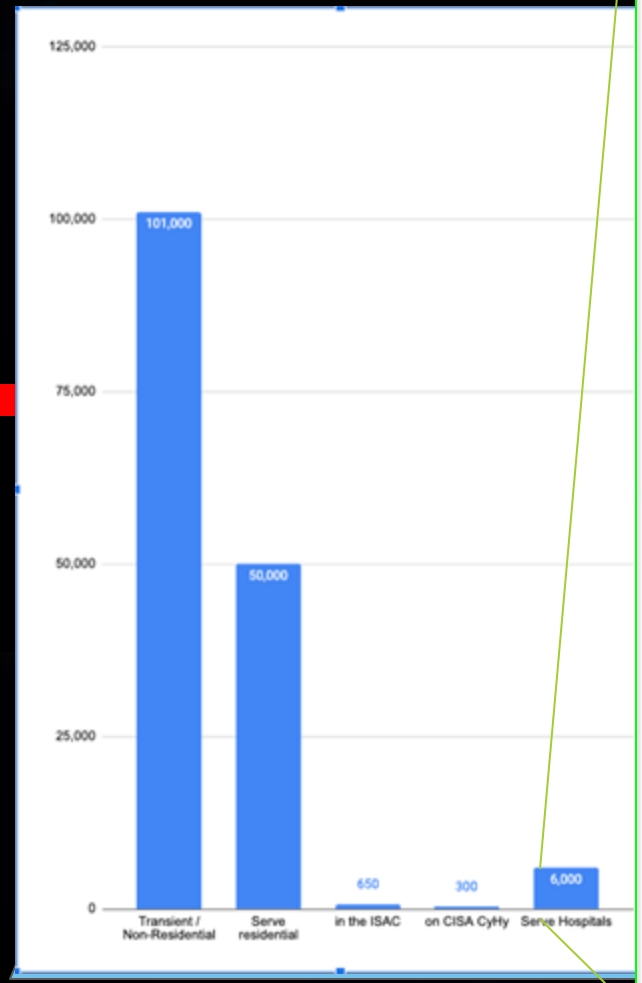


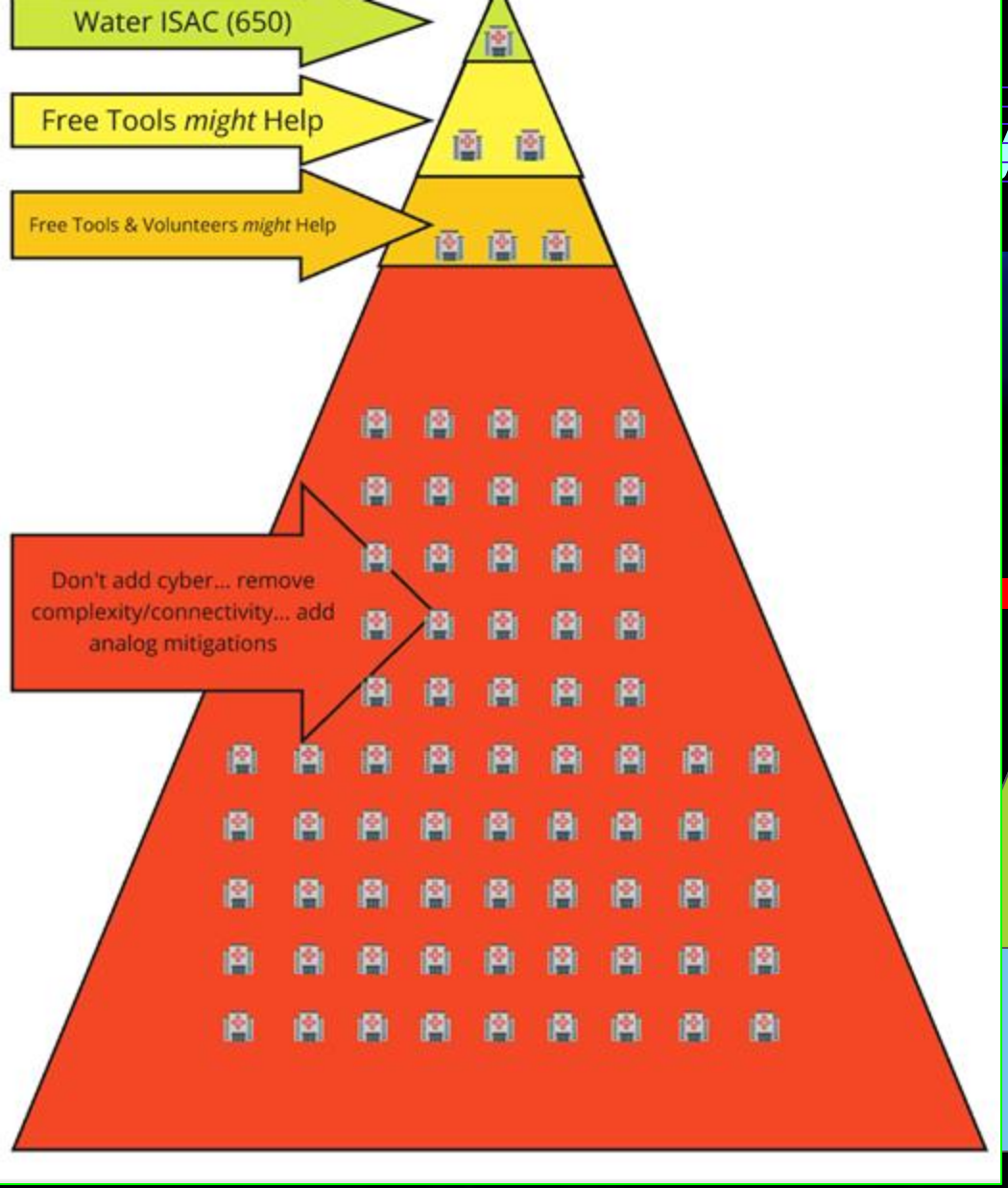
WATER

EMERGENCY CARE

ENERGY/POWER

WHICH IS ANT?

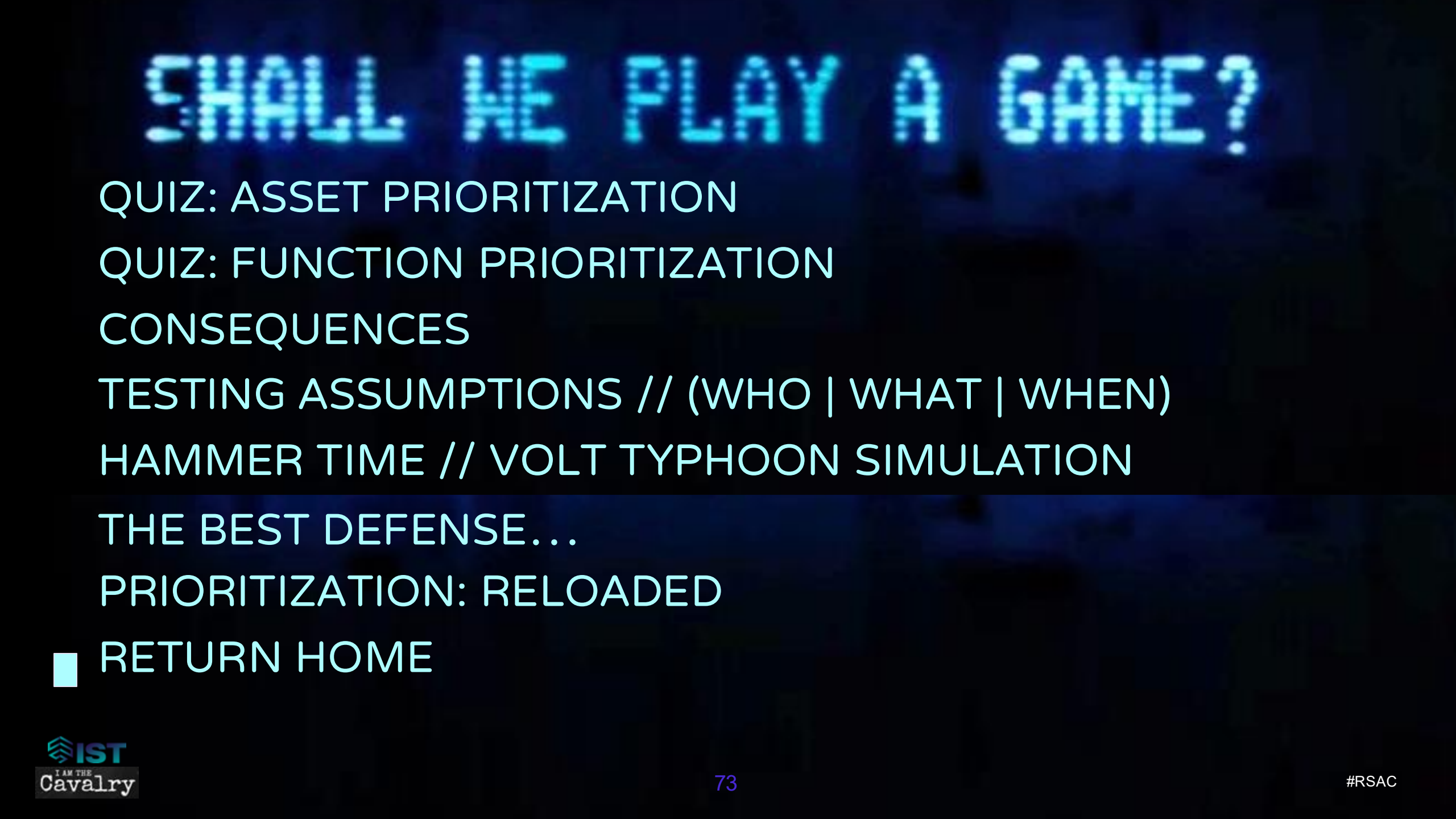



Water ISAC (650)
Free Tools *might* Help
Free Tools & Volunteers *might* Help
Don't add cyber... remove complexity/connectivity... add analog mitigations

WATER

EMERGENCY CARE

ENERGY/POWER



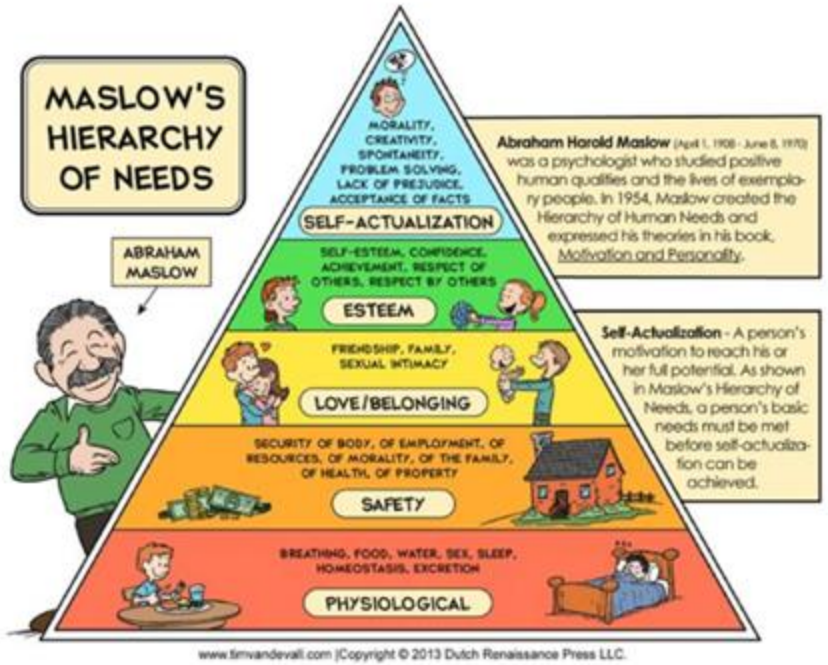
- QUIZ: ASSET PRIORITIZATION
- QUIZ: FUNCTION PRIORITIZATION
- CONSEQUENCES
- TESTING ASSUMPTIONS // (WHO | WHAT | WHEN)
- HAMMER TIME // VOLT TYPHOON SIMULATION
- THE BEST DEFENSE…
- PRIORITIZATION: RELOADED
- RETURN HOME

IST Institute for SECURITY + TECHNOLOGY

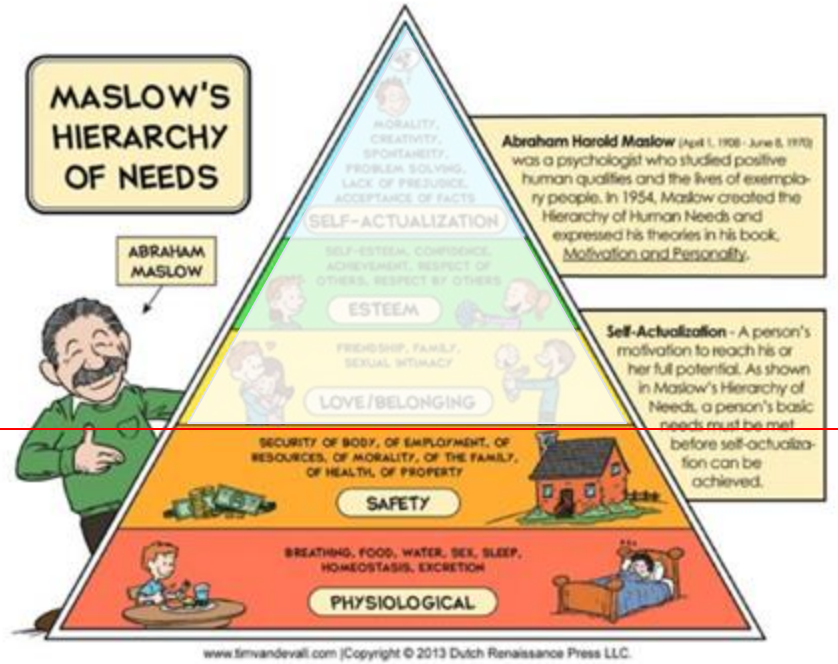
DONATE EXPLORE

IST I AM THE Cavalry

UnDisruptable27.org


MASLOW'S HIERARCHY OF NEEDS
ABRAHAM MASLOW
MORALITY, CREATIVITY, SPONTANEITY, PROBLEM SOLVING, LACK OF PREJUDICE, ACCEPTANCE OF FACTS
SELF-ACTUALIZATION
SELF-ESTEEM, CONFIDENCE, ACHIEVEMENT, RESPECT OF OTHERS, RESPECT BY OTHERS
ESTEEM
FRIENDSHIP, FAMILY, SEXUAL INTIMACY
LOVE/BELONGING
SECURITY OF BODY, OF EMPLOYMENT, OF RESOURCES, OF MORALITY, OF THE FAMILY, OF HEALTH, OF PROPERTY
SAFETY
BREATHING, FOOD, WATER, SEX, SLEEP, HOMEOSTASIS, EXCRETION
PHYSIOLOGICAL
Abraham Harold Maslow (April 1, 1908 - June 8, 1970) was a psychologist who studied positive human qualities and the lives of exemplary people. In 1954, Maslow created the Hierarchy of Human Needs and expressed his theories in his book, Motivation and Personality.
Self-Actualization - A person's motivation to reach his or her full potential. As shown in Maslow's Hierarchy of Needs, a person's basic needs must be met before self-actualization can be achieved.
www.timvandevall.com |Copyright © 2013 Dutch Renaissance Press LLC.

IST
I AM THE Cavalry


MASLOW'S HIERARCHY OF NEEDS
ABRAHAM MASLOW
Abraham Harold Maslow (April 1, 1908 - June 8, 1970) was a psychologist who studied positive human qualities and the lives of exemplary people. In 1954, Maslow created the Hierarchy of Human Needs and expressed his theories in his book, Motivation and Personality.
Self-Actualization - A person's motivation to reach his or her full potential. As shown in Maslow's Hierarchy of Needs, a person's basic needs must be met before self-actualization can be achieved.
MORALITY, CREATIVITY, SPONTANEITY, PROBLEM SOLVING, LACK OF PREJUDICE, ACCEPTANCE OF FACTS
SELF-ACTUALIZATION
SELF-ESTEEM, CONFIDENCE, ACHIEVEMENT, RESPECT OF OTHERS, RESPECT BY OTHERS
ESTEEM
FRIENDSHIP, FAMILY, SEXUAL INTIMACY
LOVE/BELONGING
SECURITY OF BODY, OF EMPLOYMENT, OF RESOURCES, OF MORALITY, OF THE FAMILY, OF HEALTH, OF PROPERTY
SAFETY
BREATHING, FOOD, WATER, SEX, SLEEP, HOMEOSTASIS, EXCRETION
PHYSIOLOGICAL
www.timvandevall.com |Copyright © 2013 Dutch Renaissance Press LLC.

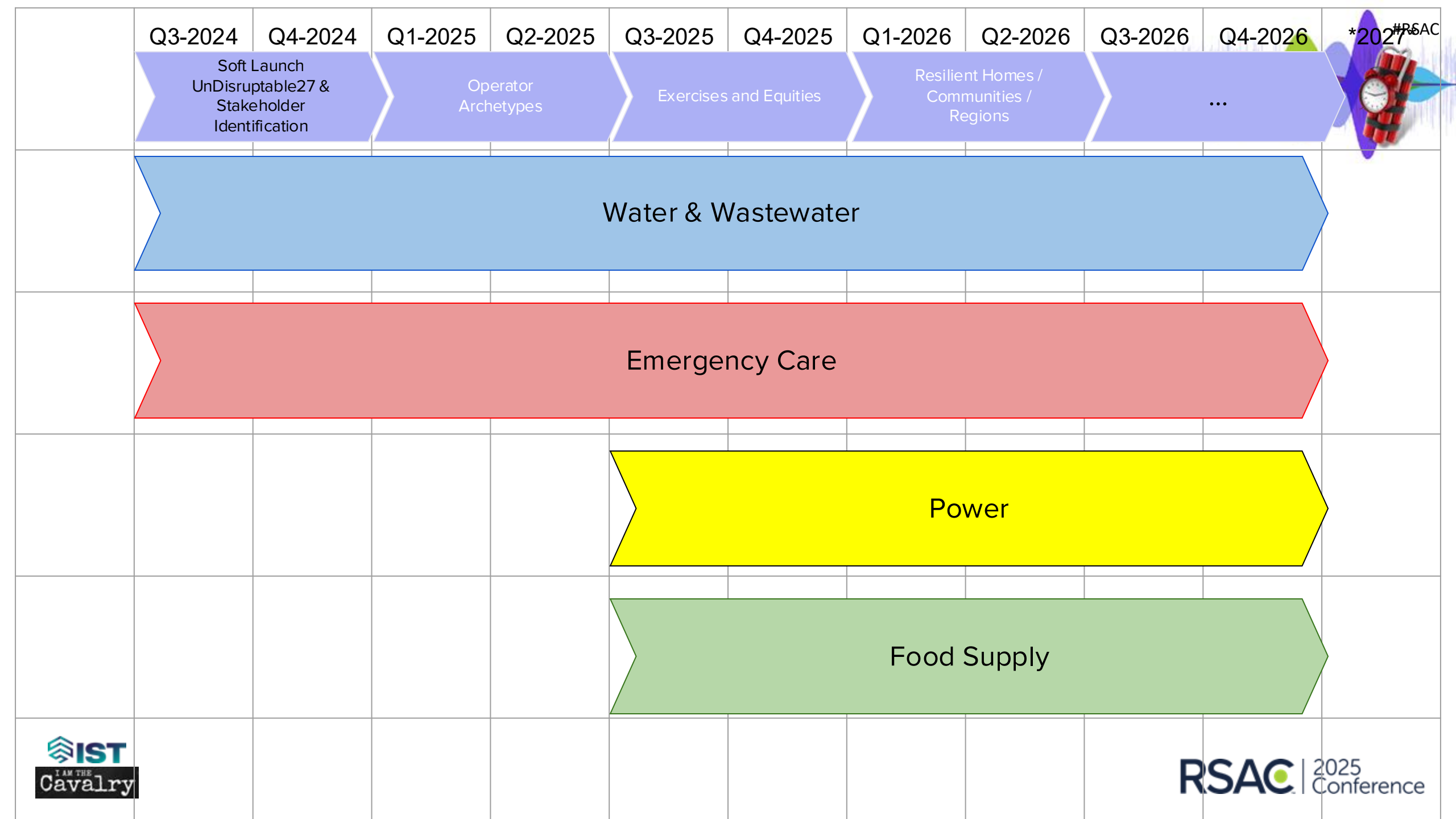
Water & Wastewater

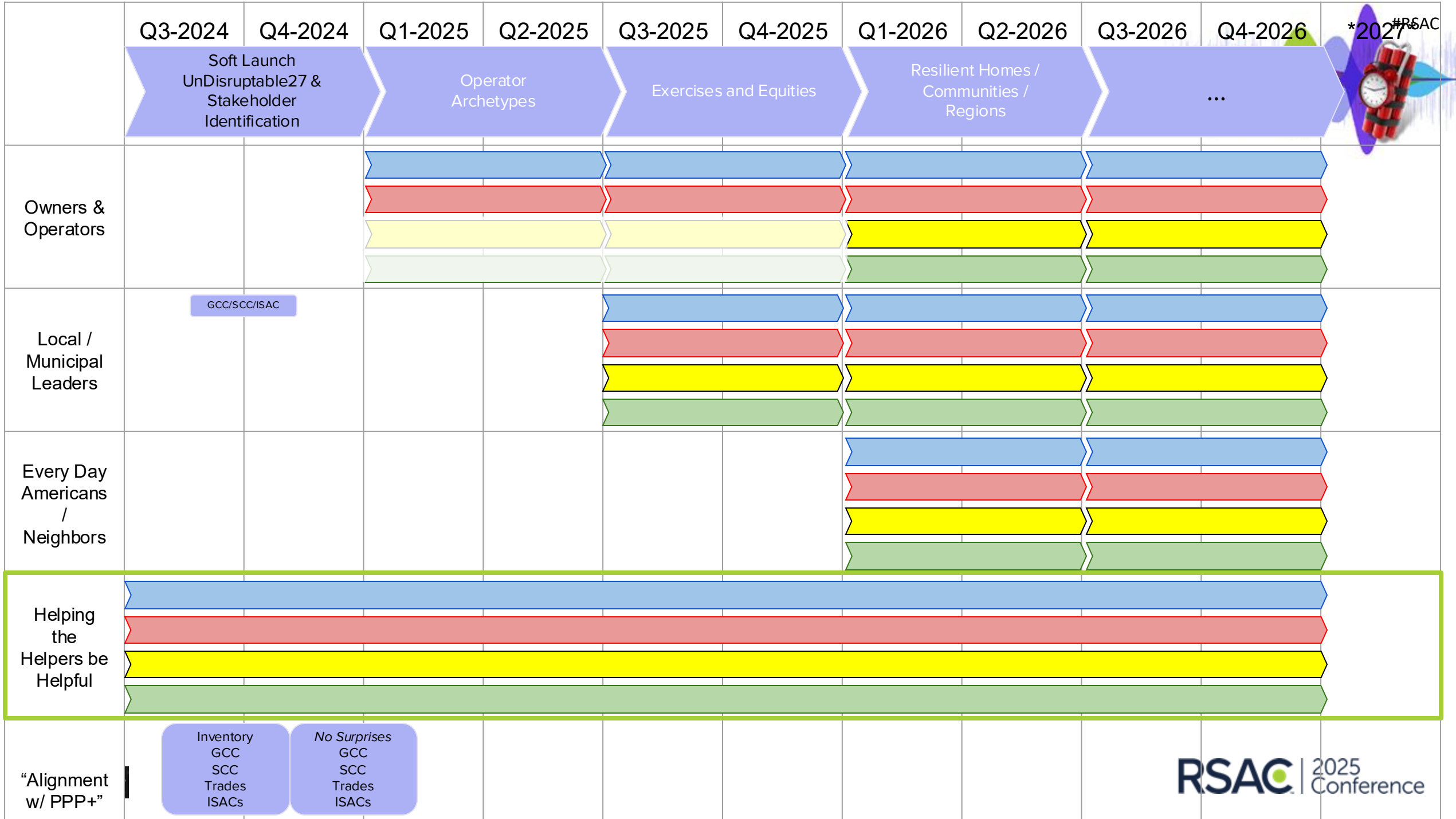
Emergency Care

Power

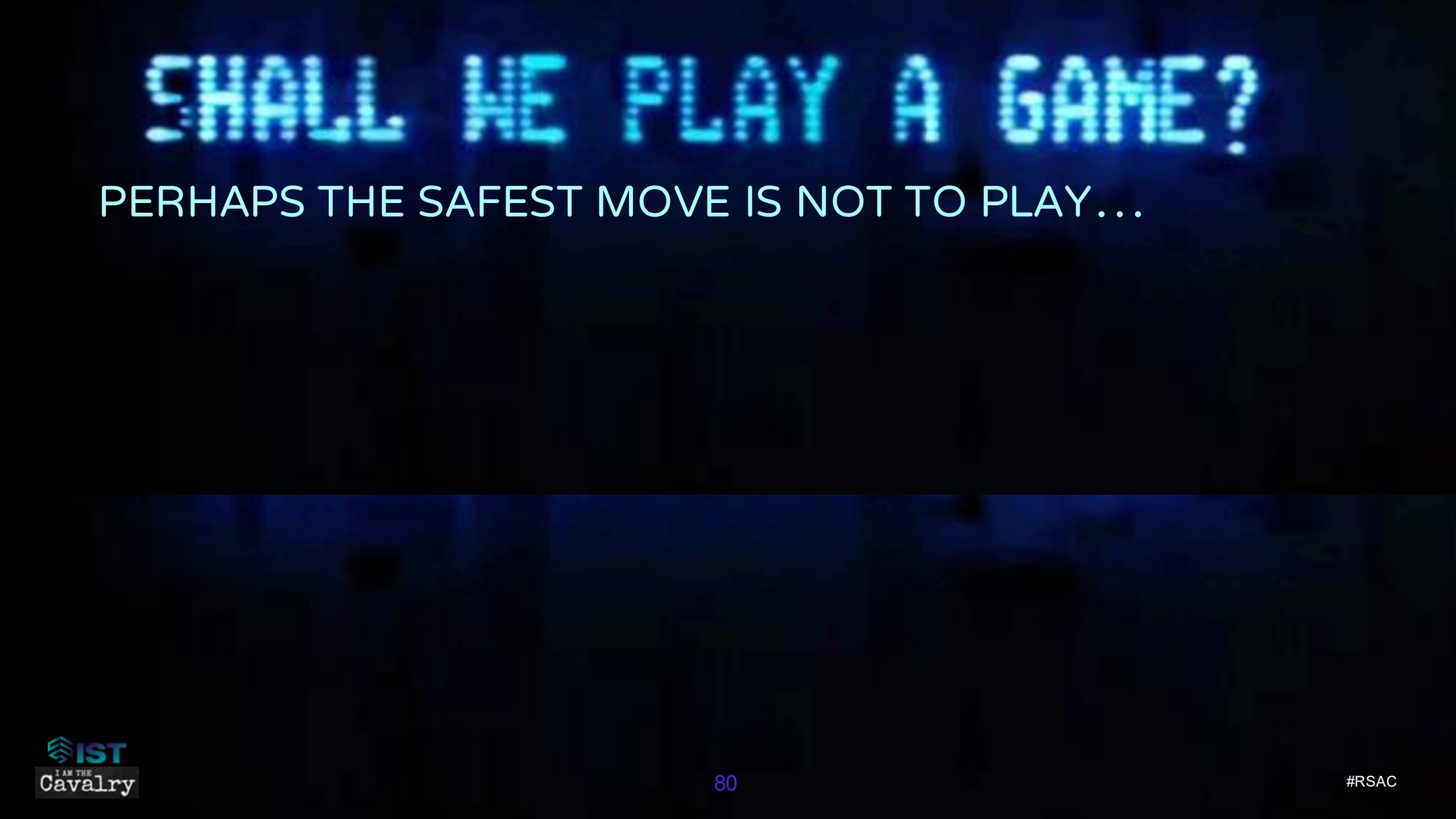
Food Supply

IST
I AM THE Cavalry

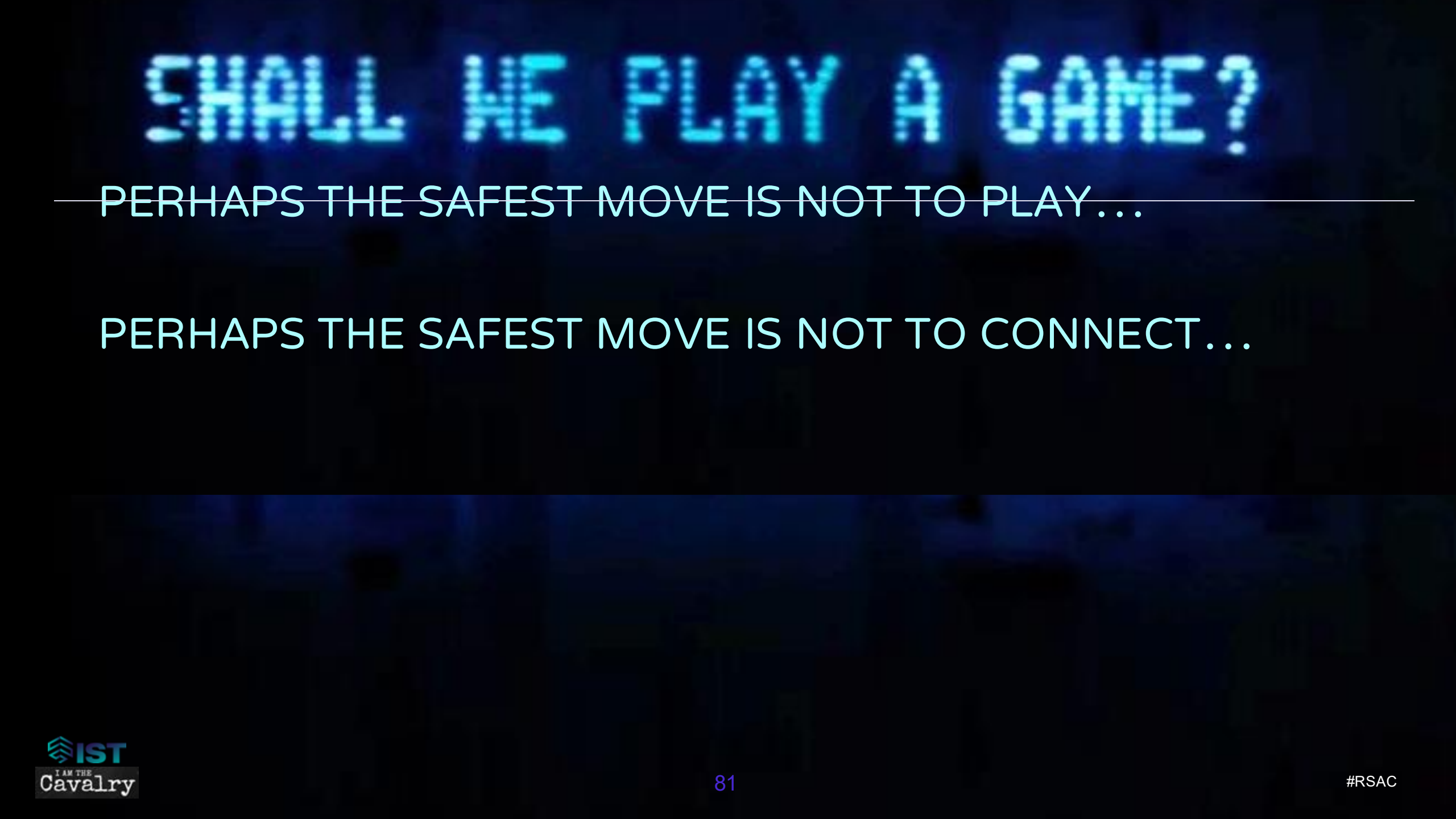

Q3-2024
Q4-2024
Q1-2025
Q2-2025
Q3-2025
Q4-2025
Q1-2026
Q2-2026
Q3-2026
Q4-2026
*2027
Soft Launch UnDisruptable27 & Stakeholder Identification
Operator Archetypes
Exercises and Equities
Resilient Homes / Communities / Regions
...
Water & Wastewater
Emergency Care
Power
Food Supply


Q3-2024
Q4-2024
Q1-2025
Q2-2025
Q3-2025
Q4-2025
Q1-2026
Q2-2026
Q3-2026
Q4-2026
*2027
Soft Launch UnDisruptable27 & Stakeholder Identification
Operator Archetypes
Exercises and Equities
Resilient Homes / Communities / Regions
...
Owners & Operators
GCC/SCC/ISAC
Local / Municipal Leaders
Every Day Americans / Neighbors
Helping the Helpers be Helpful
"Alignment w/ PPP+"
Inventory
GCC
SCC
Trades
ISACs
No Surprises
GCC
SCC
Trades
ISACs

Attendees: Our Native Talent Pool (mostly for fortune 5000)	Our communities need “left of boom” and “right of boom” *help* for resilient, continuous operations of lifelines (Water, Emergency Care, Power, Food)...	Drive enrollment for *Cyber Resilience Corps* aimed initially at *UnDisruptable27* sprint through 2025 & 2026 https://cltc.berkeley.edu/program/cyber-resilience-corps/
Vendors: Those selling products/services (mostly to fortune 2000)	These “Target Rich, Cyber Poor” owners and operators lack not just talent, but also tooling…	Public pledge to offer free (or at-cost) fit-for-purpose tools for next 2 yrs… like Dragos Community Defense, Google & MSFT Rural Hospital Programs, etc.
Speakers: The luminaries & thought leaders	Since we can’t merely do “all the best practices” & frameworks” , what is our BEST most incisive pieces of wisdom to share? *If I had 12 months to protect my water plant… If could go back 20 yrs, I’d tell my younger self ____*	Record/Edit testimonials w/ provocative questions… contacting UnDisruptable27.org

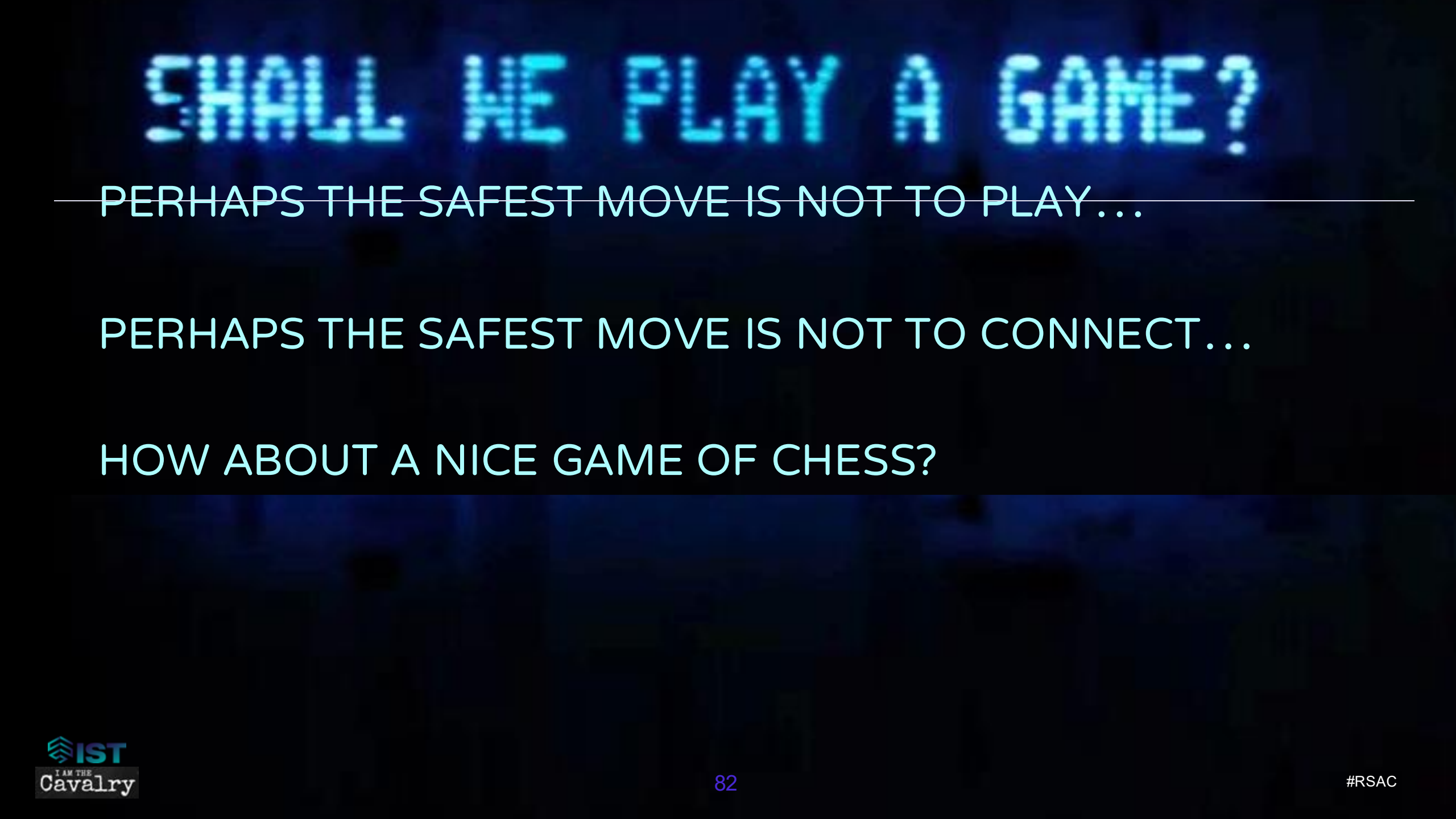


PERHAPS THE SAFEST MOVE IS NOT TO PLAY…



~~PERHAPS THE SAFEST MOVE IS NOT TO PLAY…~~

PERHAPS THE SAFEST MOVE IS NOT TO CONNECT…



~~PERHAPS THE SAFEST MOVE IS NOT TO PLAY…~~

PERHAPS THE SAFEST MOVE IS NOT TO CONNECT…

HOW ABOUT A NICE GAME OF CHESS?

I Am The Cavalry is a grassroots organization focused on the intersection of digital security, public safety, and human life.

Safer. Sooner. Together.

iamthecavalry.org

Through our **over dependence** *on* **undependable IT,** *we have created the conditions such that the actions* **any single outlier** *can have a profound and asymmetric impact on* **human life, economic, and national security.**

iamthecavalry.org

I AM THE Cavalry

RSAC 2025 Conference

…the good news is…

we have time to make changes…

…if we're focused

UnDisruptable Home & Family:
WATER:
Have X weeks of water on hand
FIltration and/or Iodine Tablets
Well?

FOOD:
Have sufficient shelf-stable food
Start a Garden (Rain Barrels)

POWER:
Generator for X Duration?
Solar options?

UnDisruptable Town/County:
5 Questions to Ask Town Council and State Leadership
Offer to Assist through lawful/protected channels:
- UnDisruptable27 Exercises
- Learn/Teach INL's Consequence Informed Engineering (CIE)
- Cyber Resilience Corps

Give Blood

UnDisruptable Country:
Call your Senators and Representatives (w/ talking points)
Create/Share playbooks for Water, Emergency Care Resilience
Spread the word about #UnDisruptable27

The Cyber Resilience Corps

What if community volunteers could protect our most under-resourced organizations?

Thousands of organizations in the U.S. remain vulnerable, overlooked by traditional cybersecurity support mechanisms focused on critical sectors like energy and transportation.

Local cyber defense initiatives—including cybersecurity clinics, volunteer programs, and state response corps—are making strides, yet they often operate independently, with limited reach.

This initiative unifies these efforts, building a cohesive, lasting support structure to protect community organizations against evolving cyber threats.

Get Involved!

- Are you part of a cyber volunteer group eager to collaborate?
- Are you a community organization in need of services?
- Are you a private company that can contribute skilled volunteers or funding?

Join our interest list:
tinyurl.com/CyberResCorps

CLTC
Center for Long-Term Cybersecurity
UC Berkeley

CyberPeace Institute

Stickers...

I WANT YOU
TO PROTECT YOUR
COMMUNITIES
UnDisruptable27.org

Apply What You Have Learned Today - 1 of 2

* Next week you should:
  - Join the UnDisruptable27 Slack
  - Assess your household's resilience to 3+ week disruptions to Water, Power, Healthcare
  - Consider volunteering in the Cyber Resilience Corps (CRC)
* In the first three months following this presentation you should:
  - Explore Consequence Informed Engineering (CIE) and lightweight Table-Tops
  - Attend Town Hall / Planning w/ "Critical Questions" RE: Lifeline Resilience
  - Identify local Owners/Operators on Water, Power, and local Emergency Care
* Within six months you should:
  - Look for "Playbooks" and Videos to better equip you help your town/county
  - Learn how your State Laws best accept and protect Good Faith / Good Samaritan in Cyber

Apply What You Have Learned Today - 2 of 2

* At work:
  - Evaluate your suite of Insurance Coverage in case of Disruption/Destruction from Volt Typhoon or similar events
  - Consider Revising/adding to your BC/DR Playbooks
    * even running a Hybrid-Conflict Table-Top to test assumptions
    * consider requirements to support your workforce for Continuity of Operation (not just the workplace)
  - Inventory your Edge Devices for those w/ excessive exposures, either:
    * Directly implicated in Volt Typhoon & Other Typhoons (E.g. TP-Link Routers)
    * UnFixed / UnFixable KEVs (Known Exploited Vulnerabilities)
    * Guilty of the CISA.gov/BadPractices
  - See if your employer may support donating some # of Security Team hours to *pro bono* Volunteerism like this effort and/or the broader CRC

THANK YOU!

@joshcorman

@iamthecavalry

I AM THE Cavalry

www.iamthecavalry.org

ABOUT IST: *The Critical Action Think Tank*

IST unites technology and policy leaders to create actionable solutions for emerging security threats.

Emerging technologies can disrupt the international balance of power. As governments compete, they shape innovation, supply chains, prosperity, and national and international security. IST shapes the incentives and alleviates the impediments to a more secure collective future.

Strategic Balancing Initiative

Dependence on digital technologies generates systemic security risks. IST works to identify incentives and mitigate digital security market failures by proposing ways to build trust, safety, and security into digital technologies from the ground up and sustain them for the future.

The Ransomware Task Force
Applied Trust & Safety
AI Foundation Model Access Initiative

Despite optimism about new technologies, some exacerbate or create existential threats to society. IST searches for solutions to the more severe risks introduced by technology, and strives to make technology itself a solution.

CATALINK
Nuclear Risk Reduction

RSAC 2025 Conference

Many Voices.
One Community.

Find #UnDisruptable27 at ICS VIllage Booth

Thank You!